

## FORSCHUNGSPROJEKT - KURZBERICHT

# AQUS

## Ausbildungs- und Qualitätsstandards für SicherheitsdienstleisterInnen

## DANKSAGUNG

Herzlichen Dank an alle Expertinnen und Experten aus akademischen Einrichtungen im In- und Ausland, Branchennetzwerken, diplomatischen Vertretungen, Bundesministerien und weiteren Behörden, Unternehmen und Organisationen, die zu den Ergebnissen dieses Projekts durch wertvolle Informationen, Einschätzungen und weitere Kontakte beigetragen haben. Unser besonderer Dank gilt dabei

- den Mitgliedern des erweiterten Projektteams als VertreterInnen der Partnerorganisationen im Projekt,
- den Teams der AußenwirtschaftsCenter der Wirtschaftskammer Österreich der im Ländervergleich untersuchten Länder,
- den GesprächspartnerInnen bei den explorativen und Leitfadent-Interviews,
- dem zuständigen Referat im Bundesamt für Verfassungsschutz und Terrorismusbekämpfung, insbesondere für die Unterstützung bei der Abwicklung der Umfrage und
- den TeilnehmerInnen an den Feedback-Gesprächen zu den vorläufigen Empfehlungen.

## IMPRESSUM

ISBN 978-3-902614-53-7

**Medieninhaberin:** FH Campus Wien – Verein zur Förderung des Fachhochschul-, Entwicklungs- und Forschungszentrums im Süden Wiens; ZVR-Zahl 625976320, DVR-Nummer: 2111102, Favoritenstraße 226, 1100 Wien.

**Redaktionsteam und für den Inhalt verantwortlich:** DI (FH) Mag. Thomas Goiser MBA MA. FH-Prof.in Mag.a Claudia Körmer, FH-Prof. DI Dr. Martin Langer; **Projektsupport:** Anna Dorfner MA; **Lektorat:** Mag.a Verena Brinda, [www.verenabrinda.at](http://www.verenabrinda.at);

**Grafik:** Doris Zemann, [www.dggd.at](http://www.dggd.at); **Druck:** GERIN, Wolkersdorf.

Die Texte und Daten wurden sorgfältig ausgearbeitet; dennoch können wir keine Haftung für die Richtigkeit der Angaben übernehmen.

**Kontakt für Feedback:** [riskmanagement@fh-campuswien.ac.at](mailto:riskmanagement@fh-campuswien.ac.at)  
Wien, Jänner 2019

## VORWORT

### Wissen und Kooperation für Sicherheit

Seit mehr als einem Jahrzehnt bilden wir an der FH Campus Wien Fachleute aus der Verwaltung, Wirtschaft, Sicherheit und Politik im Themenfeld Risiko- und Sicherheitsmanagement aus. In einigen Forschungsprojekten konnte das Team des Fachbereichs – sehr praxisnah – Grundlagenarbeit für die beteiligten Branchen leisten. Ein wachsendes Alumni-Netzwerk liefert Impulse für weitere Kooperationen.

Das KIRAS-Projekt AQUUS hat – in einer Kooperation des Fachbereichs Risiko- und Sicherheitsmanagement mit dem Zentrum für infrastrukturelle Sicherheit der Donau Universität Krems und dem Unternehmen SecureLINE – aufgezeigt, dass es eine hohe Zustimmung zu einer verpflichtenden Grundausbildung für Beschäftigte im Sicherheitsgewerbe gibt. Die erarbeiteten Empfehlungen zeigen, wie hier modular und schrittweise die Situation verbessert werden kann.

Zahlreiche Bewachungsunternehmen haben hier bereits Initiativen gesetzt und arbeiten nach anerkannten Curricula. Die Sicherheitsverantwortlichen in Unternehmen bzw. Organisationen der kritischen Infrastruktur haben hier besondere Aufmerksamkeit verdient, da sie eine hohe Verantwortung tragen. Sie sind für das Funktionieren unseres Gemeinwesens mitverantwortlich und im Ernstfall erste AnsprechpartnerInnen für Behörden. Ihre Arbeitgeber sind außerdem bedeutende Auftraggeber für sämtliche Branchen, die in irgendeiner Form mit Sicherheit zu tun haben. Durch ihr Handeln – insbesondere bei Beschaffungsvorgängen – setzen die Sicherheitsverantwortlichen Trends und lenken ihre Dienstleistenden zur Entwicklung neuer Angebote.

Eines ist klar: Das Thema Sicherheit wird weiter an Bedeutung gewinnen und sich durch Globalisierung und Digitalisierung in den nächsten Jahrzehnten rapide verändern. Ohne unsere Partner aus anderen Hochschulen, Bundesministerien, Spezialbehörden, Landesverwaltungen, Institutionen und Unternehmen wäre eine Bewältigung dieser Veränderungen nicht möglich. Stärkere Kooperation und Vernetzung bringen uns weiter.



FH Campus Wien Schedl

Univ.-Prof. Dr. Arthur Mettinger  
Leiter des Departments  
Public Sector,  
Vizekanzler für Lehre der  
FH Campus Wien

## INHALTSVERZEICHNIS

Executive Summary	Seite 5
Projektverlauf	Seite 6
Partner-Statements	Seite 8
Ergebnisse der Umfrage	Seite 10
Empfehlungen	Seite 26
Nachwort und Ausblick	Seite 34
Das AQUUS Team	Seite 35

## EXECUTIVE SUMMARY

The AQUUS project surveyed current approaches to and future perspectives for training and quality standards for security service providers. This KIRAS project was implemented as a research service by a project team under the direction of the Section of Risk and Corporate Security Management of the University of Applied Sciences FH Campus Wien in cooperation with the Center for Infrastructural Security of the Danube University Krems and SecureLINE, an Austrian company offering training courses for those working in the security industry. The project aimed at elaborating recommendations for training and quality standards for security companies. The wide range of the sectors involved constituted a special challenge. According to its definition, the project extended to the „traditional“ security industry (professional detectives and security companies) as well as in-house security service providers of companies and consultants in the fields of risk management (RM), business continuity management (BCM) and security management (SM) and IT security service providers. Due to this variety, there are, of course, different preconditions and training requirements for practicing these professions and various career opportunities.

The project was initiated on 1 October 2017 and was subdivided into four work packages:

- WP1: project management/controlling tasks
- WP2: analysis of the status quo/basics
- WP3: needs analysis/empirical part
- WP4: recommendations/harmonisation of the proposals

The methods applied included desk research, qualitative expert interviews with different stakeholders and, for the first time, a quantitative online survey among critical infrastructure companies and organisations.

A comparison of country data has shown that Austria is lagging behind, as there are no (minimum) training requirements for employees of security companies. All the other countries have made progress in this respect, albeit to varying extents, and they have made different experiences. Interesting ideas which could be adapted to the situation in Austria and then implemented mainly come from Germany and Switzerland.

According to the survey, those responsible for the security and safety of critical infrastructure expect an increase in the incidence of all the threats mentioned in the survey, including corporate and industrial espionage, sabotage, violence motivated by extremism, etc. Almost all those surveyed approve of a mandatory training for employees in the security industry.

The 18 recommendations elaborated in the course of the project are assigned to four fields:

- A labour market and working conditions
- B training and further training
- C procurement and standardisation
- D communication and awareness-raising

The industries in this sector may become actively involved in elaborating quality standards, some of which have not yet been defined. At the latest when they will have proven useful in practice, will those quality standards become widely accepted. As a first step, it is proposed to start registering all relevant training and further training offers and developing voluntary certifications for security consultants. The Austrian Network and Information Systems Security Act was only addressed to a limited extent as it was still in the final stages before adoption at the end of the project period.

In addition to initiatives within the industry and standardisation processes, the elaboration of legislative acts at the federal level is proposed in some respects (e.g., as part of the amendment of the Austrian Weapons Act or on the occasion of the issuance of a statutory training order for the security industry, whose scope goes beyond previous proposals).

The recommendations proposed by the project may be implemented individually or in various combinations and are intended to contribute to a continuous improvement of the security situation of Austria's critical infrastructure.

## EXECUTIVE SUMMARY

Im Projekt AQUUS wurden aktuelle Einstellungen und Perspektiven zu Ausbildungs- und Qualitätsstandards für SicherheitsdienstleisterInnen erhoben. Umgesetzt wurde dieses KIRAS-Projekt als Forschungsdienstleistung von einem Projektteam unter der Federführung des Fachbereichs Risiko- und Sicherheitsmanagement der FH Campus Wien gemeinsam mit dem Zentrum für infrastrukturelle Sicherheit der Donau Universität Krems und dem Ausbildungsunternehmen SecureLINE. Dabei wurden abgestimmte Empfehlungen für Ausbildungs- und Qualitätsstandards für Sicherheitsunternehmen entwickelt.

Die Breite der betroffenen Branchen stellte eine besondere Herausforderung dar. Von der Ausgangsdefinition des Projekts umfasst neben dem „klassischen“ Sicherheitsgewerbe (Berufsdetektive/Berufsdetektivinnen und Bewachungsunternehmen), auch In-House-SicherheitsdienstleisterInnen von Unternehmen sowie BeraterInnen in den Bereichen Risikomanagement (RM), Business Continuity Management (BCM) und Sicherheitsmanagement (SM) und IT-SicherheitsdienstleisterInnen. Entsprechend breit gefächert sind die unterschiedlich geregelten Berufszugänge, Ausbildungen und Karrieremöglichkeiten.

Das ab 1. Oktober 2017 laufende Projekt war in vier Arbeitspakete gegliedert:

- AP1: Projektmanagement/Steuerungsaufgaben
- AP2: Ist-Analyse/Grundlagenüberblick
- AP3: Bedarfsanalyse/empirischer Teil
- AP4: Empfehlungen/Harmonisierung der Vorschläge

Die eingesetzten Methoden umfassten „desk research“, eine qualitative Befragung von ExpertInnen bei unterschiedlichen betroffenen Stakeholdern sowie eine – erstmals in dieser Form durchgeführte – quantitative Online-Umfrage bei den Unternehmen bzw. Organisationen der kritischen Infrastruktur.

Der Ländervergleich zeigte, dass Österreich zurückbleibt, da keine verpflichtende (Mindest-)Ausbildung für Beschäftigte bei Bewachungsunternehmen existiert. Sämtliche untersuchte Länder sind hier weiter fortgeschritten, wenn auch in unterschiedlichem Ausmaß, und haben unterschiedliche Erfahrungen gemacht. Interessante Anleihen zur angepassten Umsetzung in Österreich liefern vor allem die Schweiz und Deutschland.

Für die kommenden Jahre erwarten die Sicherheitsverantwortlichen der kritischen Infrastruktur laut der Umfrage durchwegs eine höhere Betroffenheit von sämtlichen abgefragten Bedrohungen wie Wirtschafts- und Industriespionage, Sabotage, durch Extremismus motivierte Gewalt etc. Nahezu sämtliche Befragte befürworten eine verpflichtende Ausbildung für Beschäftigte im Sicherheitsgewerbe.

Die im Projekt erarbeiteten 18 Empfehlungen sind in vier Handlungsfelder gegliedert:

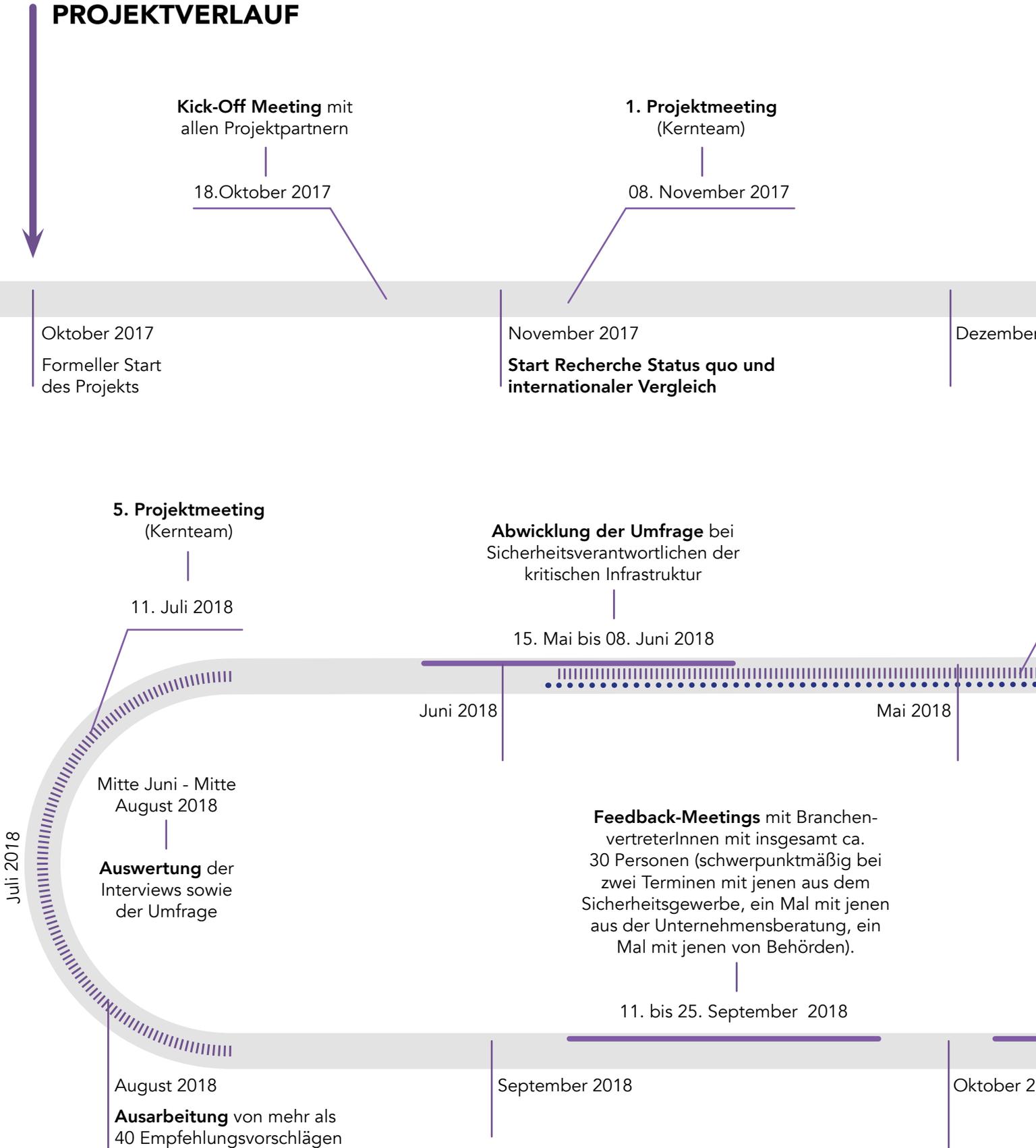
- A Arbeitsmarkt und Arbeitsbedingungen
- B Aus- und Weiterbildung
- C Beschaffung und Normierung
- D Kommunikation und Bewusstseinsbildung

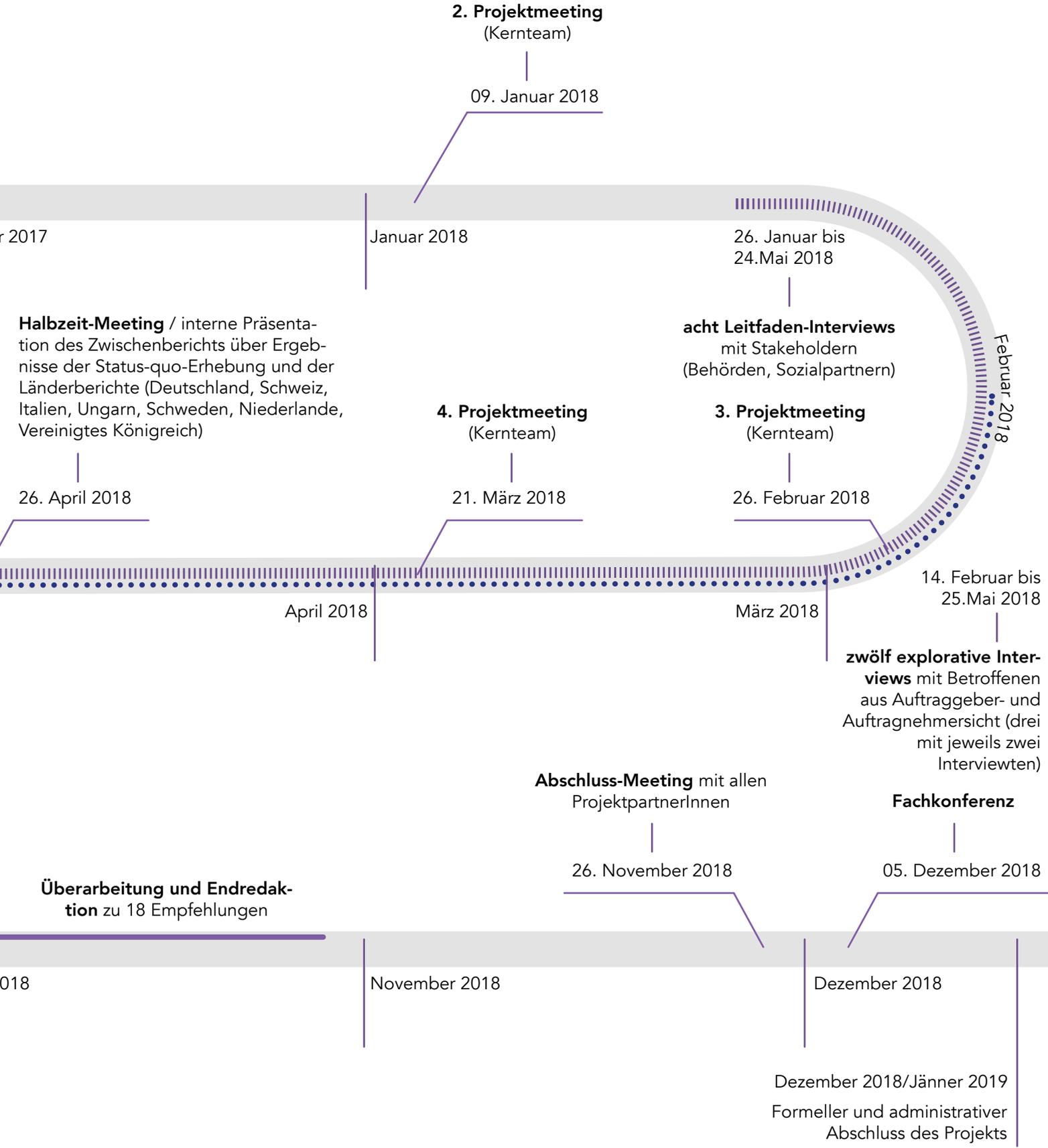
Die teilweise erst zu schaffenden Qualitätsstandards können so von den betroffenen Branchen selbst mitentwickelt werden und werden – spätestens nach erwiesener Eignung – entsprechende Akzeptanz erfahren. Dabei wird als erster Schritt zumindest eine Registrierung für sämtliche einschlägige Aus- und Weiterbildungsangebote und die Entwicklung von freiwilligen Zertifizierungen für SicherheitsberaterInnen angeregt. Durch die erst zu Projektende eingeleitete Verwirklichung eines NIS-Gesetzes wurde dieser Themenstrang entsprechend nur in geringerem Ausmaß behandelt.

Neben Brancheninitiativen und Normierungsverfahren werden in Einzelfällen auch Akte der Rechtsetzung auf bundespolitischer Ebene angeregt (z.B. im Rahmen der Novelle des Waffengesetzes oder im Rahmen der Erlassung einer Ausbildungsverordnung für das Sicherheitsgewerbe, die etwas über bisherige Vorschläge hinausgeht).

Die im Projekt vorgeschlagenen Empfehlungen sind sowohl isoliert, als auch kombiniert umsetzbar und sollen dazu beitragen, die Sicherheitslage in Bezug auf Österreichs kritische Infrastruktur weiter zu verbessern.

# PROJEKTVERLAUF





## PARTNER-STATEMENTS

Österreich verfolgt eine proaktive und umfassende Sicherheitspolitik mit dem Ziel, die freie Entfaltung der Menschen zu ermöglichen und zum gesellschaftlichen Zusammenhalt beizutragen. Dazu braucht es auch eine leistungsfähige, gesamtstaatliche Sicherheitsorganisation und ein enges Zusammenwirken aller Beteiligten. All jene, die für Sicherheit im Einsatz sind, müssen bestmögliche Rahmenbedingungen zur Aufgabenerfüllung vorfinden.



Bundeskanzleramt

Private Sicherheitsdienstleister erfüllen angesichts stetig steigender Herausforderungen zur Gewährleistung eines hohen Sicherheitsniveaus zunehmend wichtige Aufgaben im Rahmen der gesamtstaatlichen Sicherheitszusammenarbeit. Die Festlegung entsprechender Qualitäts- und Ausbildungsstandards auch in diesem Bereich ist daher eine wesentliche Zielsetzung. Das Projekt AQUUS leistet einen wichtigen Beitrag in diesem Zusammenhang.

**Mag. Dr. Helmut Schnitzer,**  
Bundeskanzleramt, Leiter der  
Abteilung IV/7: Sicherheitspolitik,  
Justiz und Inneres

Der Bedarf an privaten Sicherheitsdienstleistungen ist auch wegen neuer Bedrohungsbilder durch Digitalisierung sowie Extremismus und Terrorismus stark gestiegen. Standards dafür sollten in Österreich und zahlreichen anderen Ländern Europas noch besser definiert werden.

Gegenüber Betreibern kritischer Infrastruktur ist der öffentliche Anspruch an das Sicherheitsniveau naturgemäß sehr hoch. Sie müssen Gefahren abschätzen können, eigene Maßnahmen setzen und die Sicherheitsbehörden rechtzeitig einbinden – Fähigkeiten, die jedenfalls teilweise durch private Sicherheitsdienstleister erbracht werden.

Dass die vorliegende Studie sowohl die Anforderungen von BehördenvertreterInnen als auch die Erfahrungen und Erwartungen von Betreibern kritischer Infrastruktureinrichtungen berücksichtigt, ist eine nützliche Grundlage für den weiteren Diskurs.

**Dr.<sup>in</sup> Michaela Kardeis, Generaldirektorin**  
für die öffentliche Sicherheit



BWf, Pachauer, 2018

In Österreich fehlen nach wie vor jegliche einheitlichen Vorgaben, wie Beschäftigte im Bewachungsgewerbe auszubilden sind. Wir sind damit Schlusslicht in Europa – und das in einer Branche, die eine immer wichtigere Rolle in der Sicherheitsarchitektur des Landes einnimmt.

Trotz vollen Konsenses zwischen WKO, BMI, VIDA und VSÖ über eine entsprechende Ausbildungsordnung im Gewerberecht hemmt die Politik seit Jahren die Umsetzung. Dabei sind die Inhalte mehr als nur logisch und notwendig:

- Zwingende einheitliche Basisausbildung in zugelassenen Ausbildungsinstituten mit Abschlussprüfung
- Ausweistragepflicht: Ausweise für jene Beschäftigten, die Schulung und Prüfung erfolgreich absolviert UND eine aktuelle positive sicherheitspolizeiliche Überprüfung haben
- Evidenzhaltung aller zugelassenen MitarbeiterInnen und Information an die Sicherheitsunternehmen bei Verlust der Zuverlässigkeit

**Mag. Martin Wiesinger, Präsident des Verbands der**  
Sicherheitsunternehmen Österreichs  
**Mag. Thomas Forstner, Generalsekretär des Verbands der**  
Sicherheitsunternehmen Österreichs



Ludwig Schedl



VSOE

Die Gesellschaft verändert sich, der Umgang unter den Menschen wird immer rauer und konflikträchtiger. Daher ist neben dem fachlichen Wissen vermehrt auch das adäquate Verhalten zu vermitteln. In unserem Bildungszentrum SICHERHEIT beträgt der Anteil von Unterricht zu Konfliktmanagement und Deeskalation heute bereits über 50 %.

Gerade im Bereich kritischer Infrastrukturen und dort, wo viele Menschen Räume gemeinsam nutzen (öffentlicher Verkehr, Veranstaltungen), braucht es moderne und maßgeschneiderte Ausbildungs- und Qualitätsstandards. Denn neben der Rekrutierung und Führung von MitarbeiterInnen stellt deren Aus- und Weiterbildung die dritte wesentliche Säule für die Qualität in allen Sicherheitsberufen dar. Mit AQUS ist ein wesentlicher Baustein für weitere Schritte großartig gelungen.



Michael Zoratti, MSc

SecureLINE

Herausforderungen im Sicherheitsbereich sind heute komplexer, stärker miteinander vernetzt und vor allem weniger vorhersehbar als bisher. Der Schutz kritischer Infrastruktur ist daher als gesamtstaatliche Aufgabe zu sehen und bedarf des harmonischen Zusammenspiels aller Stakeholder. Die permanente Weiterentwicklung von Strategien wie auch der jeweiligen „unternehmens-(strategischen) Konzepte“ stellt eine der wesentlichsten Voraussetzungen hierfür dar. Als Herausforderung kann das unabhängige Entwickeln bzw. Adaptieren von Bedrohungsanalysen, Aus- und Weiterbildungsabläufen inklusive einer umfassenden Qualitätssicherung gesehen werden. Ein wesentlicher Schritt in die richtige Richtung wurde durch das gegenwärtige Projekt, aber auch durch die Implementierung der Schule für Führung und Sicherheit - als Umsetzung eines Leuchtturmprojektes gemäß Regierungsübereinkommen - gesetzt. All diese Maßnahmen sind im Lichte „Sicherheit für Österreich kann nicht früh genug beginnen“ zu sehen.

**Bgdr. Mag. Anton Wessely, Leiter Ausbildungsabteilung A, derzeit Stabschef des Bundesministers im BMLV**



BMLV



DUK



Andrea Reischer

**Ass.-Prof. Mag. Dr. Walter Seböck, MSc, MBA  
Bettina Pospisil, BA, MA**

Als Universität für Weiterbildung freuen wir uns, gemeinsam mit den InitiatorInnen des Projekts, mit dem Projekt AQUS einen wichtigen Meilenstein zur Standardisierung der Aus- und Weiterbildung im privaten Sicherheitsbereich legen zu können. Die aus dem Projekt heraus entwickelten Empfehlungen zeigen die wichtigsten Handlungsfelder auf und ermöglichen es, den privaten Sicherheitsbereich am Standort Österreich zu verbessern und zu standardisieren.

Auch wir als Zentrum für Infrastrukturelle Sicherheit der Donau-Universität Krems werden unseren Teil für das Vorantreiben der Aus- und Weiterbildung im Sicherheitsbereich beitragen. So werden wir die neuen Erkenntnisse durch das Projekt AQUS in unser bestehendes Lehrangebot integrieren und bei zukünftigen Kooperationen in Lehre und Forschung gezielt verfolgen. Wir freuen und bedanken uns, dass wir gemeinsam mit den InitiatorInnen des Projekts AQUS an diesem wichtigen Projekt mitarbeiten konnten und werden auch in Zukunft Ausbildungs- und Qualitätsstandards im privaten Sicherheitsbereich begleiten.

Sicherheit ist auf der einen Seite von fundamentaler Bedeutung für die österreichische Wirtschaft und Gesellschaft. Auf der anderen Seite ist die Gewährleistung von Sicherheit ein komplexer Vorgang, in den Behörden, gewerbliche Sicherheitsdienstleister sowie Unternehmen mit strategischer Relevanz für das Funktionieren des Wirtschaftsstandortes Österreich eingebunden werden müssen.

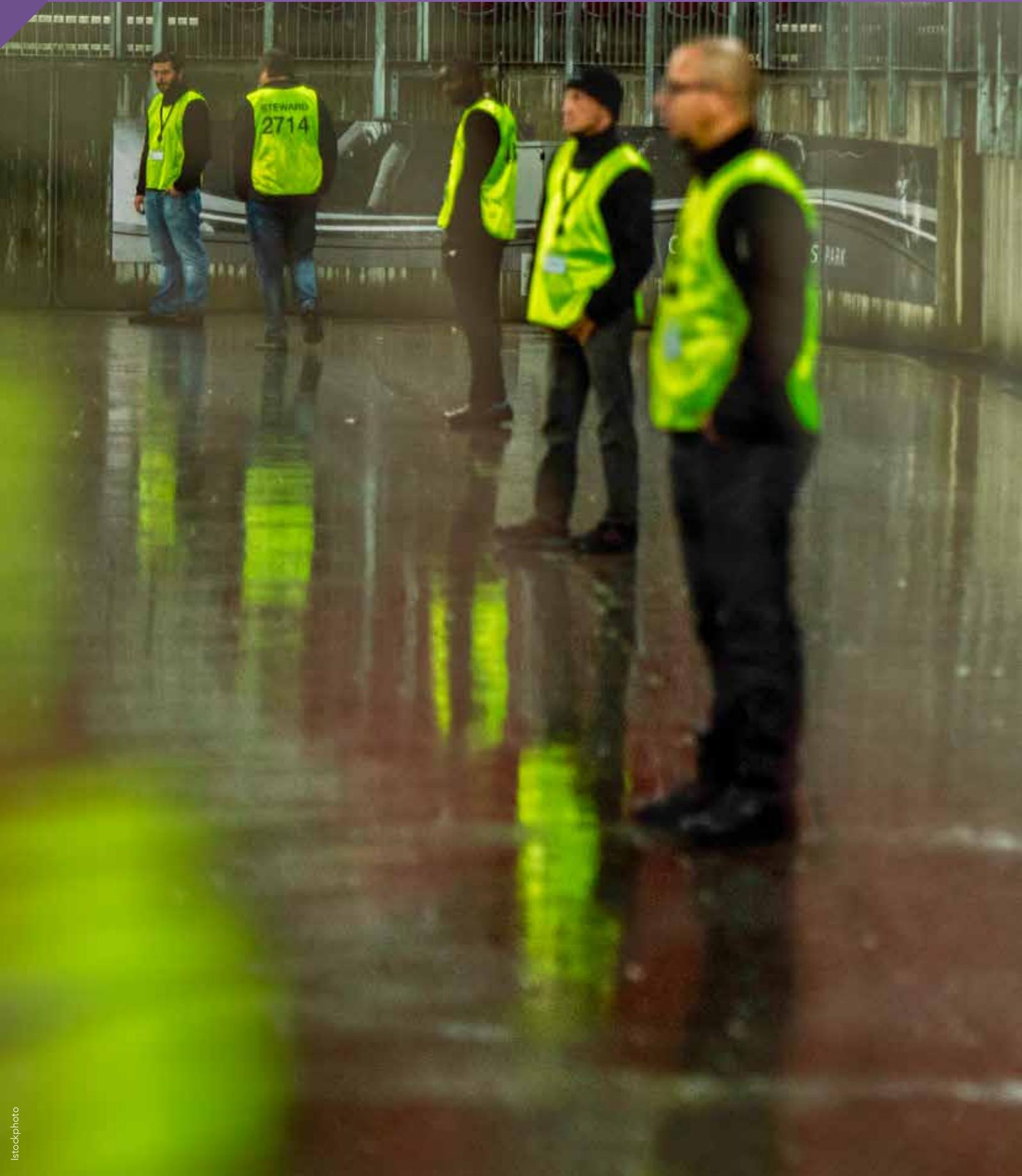
Es ist den InitiatorInnen des Projektes dafür zu danken, dass sie die durchaus divergierenden Bedürfnisse dieser Stakeholder systematisch identifiziert und einem internationalen Vergleich unterzogen haben. Die Wirtschaftskammer Österreich hat daher das Projekt AQUS durch die Bereitstellung hochqualitativer Daten und methodischen Know-hows gerne unterstützt.

**Dr.<sup>in</sup> Ulrike Oschischnig, Leiterin  
Stabsabteilung Statistik der WKÖ**



WKÖ

# ERGEBNISSE DER UMFRAGE



## WICHTIGSTE ERGEBNISSE

Insgesamt 71 von 377 Kontakten des Bundesamts für Verfassungsschutz und Terrorismusbekämpfung (BVT) aus der kritischen Infrastruktur antworteten im Mai/Juni 2018 auf die anonyme Umfrage, woraus sich eine Teilnahmequote von 18,8 % ergibt. Sämtliche Bereiche der kritischen Infrastruktur waren unter den Antworten vertreten (wobei auch möglich war, dass aus einzelnen Unternehmen/Organisationen mehrere Antworten eingegangen sind).

Der Bedarf an Präventions- und Schutzmaßnahmen scheint gegeben: Wo diese als relevant angesehen werden, sehen die Befragten für den Zeitraum bis 2022 einen potenziellen Anstieg sämtlicher abgefragten Bedrohungen – am stärksten durch IT-Angriffe (100 %; Kombination der Antworten von „stark steigen“ und „eher steigen“), Social Engineering (92,8 %), weltanschaulich und politisch motivierten Extremismus/Terrorismus (74,2 %), Spionage (67,2 %), Eigentumskriminalität (58,1 %) und Gewalthandlungen (jeweils 48,4 %).

### Sicherheit intern und extern organisiert

Die Tätigkeit als Sicherheitsverantwortliche/r ist überwiegend eine Nebenaufgabe oder ein Vollzeitjob (keine Halbtagsaufgabe). Aus den Antworten ist ein großes Bemühen um die Aufgabe, Kooperativität und Verbesserung der Situation ersichtlich.

Die Implementierung von Normen und Standards erweist sich als wichtige (Dauer-) Aufgabe und Zeichen von immer stärkerer Professionalisierung. In vielen Fällen

werden sowohl interne, als auch externe Kräfte für Sicherheitsaufgaben eingesetzt. Bei internen MitarbeiterInnen ist oft eine kombinierte Ausbildung vorgesehen, für die interne und externe TrainerInnen eingesetzt werden. Die Befragten setzen externe Kräfte hauptsächlich im Wachdienst und im Service und Sicherheitsdienst ein. Sie befürworten überwiegend verbindliche Ausbildungsstandards bei Bewachungsunternehmen. In vielen Fällen existieren bereits besondere Qualifikationsstandards für das eingesetzte Personal. Ausschreibungen sind das am weitesten verbreitete Mittel, um diese festzulegen. Wichtige Themen dabei sind Ausbildung, Branchenerfahrung und Zuverlässigkeitsnachweise.

### Gefragt und gefordert: Unterstützung durch Behörden und Private

Wenn externe Beratungsdienstleistungen in Anspruch genommen werden, sind sie als AuftraggeberInnen zufrieden bis sehr zufrieden. Für die Zukunft orten die Befragten generell hohen Bedarf an Beratung. Seitens der Befragten werden die Serviceleistungen von BMI und BVT bzw. LVTs immer wieder in Anspruch genommen und im Vergleich mit anderen Beratungsangeboten hoch geschätzt. Durch Ausschreibungen lässt sich die Qualität von externen Dienstleistungen sehr gut steuern; gleichzeitig haben sie Signalwirkung für andere. Wichtige Themen dabei sind Ausbildung, Branchenerfahrung und Zuverlässigkeitsnachweise.

Einheitliche Ausbildungsstandards bei Bewachungsunternehmen werden deutlich befürwortet.

## METHODISCHES VORGEHEN UND ORGANISATION DER UMFRAGE

Die Gestaltung des Fragebogens erfolgte in mehreren Runden zuerst durch das Projekt-Kernteam im Zeitraum Februar und März 2018. Alle ProjektmitarbeiterInnen und ausgewählte weitere Kontakte wurden nach der Projekt-Zwischenpräsentation am 26. April 2018 zu einem Pretest mit einer elektronischen Testversion des Fragebogens eingeladen und konnten direkt Feedback einbringen. Die Fragebögen inklusive Feedback wurden in der Folge evaluiert, und die Vorschläge wurden überwiegend eingearbeitet. Die technische Umsetzung erfolgte über die Plattform SoSci Survey zur Erstellung von Onlinefragebögen.

Am 15. Mai wurde der Link der Online-Umfrage mit einem Anschreiben seitens des BVT an 377 E-Mail-Adressen versandt. Diese direkten AnsprechpartnerInnen des BVT bei Unternehmen bzw. Organisationen der kritischen Infrastruktur werden je nach Kontaktfrequenz und Betreuungintensität in „A- und B-Kontakte“ eingeteilt. Der Versand eines Reminders erfolgte am 30. Mai wiederum per E-Mail an sämtliche Kontaktadressen. Aufgrund der IP-Adressen wurde eine individuelle Antwort ermöglicht (mit Speichermöglichkeit), die Adressen waren für die Projektleitung

nicht einsehbar. Die Antworten erfolgten anonym. Teilnehmerverhalten: Insgesamt begannen 135 Personen mit der Beantwortung (35,8 % der angeschriebenen Kontakte). Abgeschlossen wurden 71 Interviews, die Gegenstand der folgenden Auswertung sind. Damit ergibt sich eine Teilnahmequote von 18,8 % der kontaktierten Personen. Dies ist für eine Umfrage in einem sensiblen Bereich wie Sicherheit ein hoher Wert. Die folgende Aufbereitung der Umfrageergebnisse orientiert sich mit wenigen Ausnahmen aus redaktionellen Gründen an der Reihenfolge im Fragebogen.

Wichtige Anmerkungen: Bisher hat das BVT keine Umfragen bei den Kontakten aus Unternehmen bzw. Organisationen der kritischen Infrastruktur durchgeführt bzw. unterstützt. In einigen Organisationen verfügt das BVT über mehrere Ansprechpersonen. Daher ist nicht ausgeschlossen, dass aus manchen Organisationen auch mehrere Antworten eingelangt sind. Insofern liefern die Antworten zwar ein qualifiziertes Stimmungsbild, es sind aber keine Aussagen hinsichtlich Anzahl der Organisationen bzw. Unternehmen möglich.

## ZUSAMMENSETZUNG DER ANTWORTENDEN, ORGANISATORISCHE FRAGEN

### Verteilung der Antwortenden nach Branchen

Die Antwortoptionen dieser Frage folgten der vom Bundeskanzleramt und dem BVT verwendeten Aufgliederung der kritischen Infrastruktur. Es antworteten Personen aus allen Segmenten.

Je 15,5 % der Antwortenden gaben die Bereiche Finanzen, Chemische Industrie und Gesundheit an, gefolgt von Informations- und Kommunikationstechnologien (12,7 %), Verfassungsmäßige Einrichtungen und Energie (je 8,5 %).

7 % der Antwortenden kommen aus dem Sektor Transport/Verkehr 4,2 % aus dem Sektor „Lebensmittel“. Je ein Kontakt (entspricht 1,4 %) ordnete sich dem Segment „Forschungseinrichtungen“, „Sozial- und Verteilssysteme“ oder gar nicht zu. Die Kontakte unter „Sonstiges“ umfassten Selbstbezeichnungen wie „Druckerei“, „Meteorologie“, „Universität“ etc. Auf eine nachträgliche Zuordnung zu den offiziellen Kategorien im Zuge der Auswertung wurde verzichtet, da diese willkürlich wäre.

In welchem der folgenden Bereiche ist Ihr Unternehmen bzw. Ihre Organisation vor allem tätig?

N=71

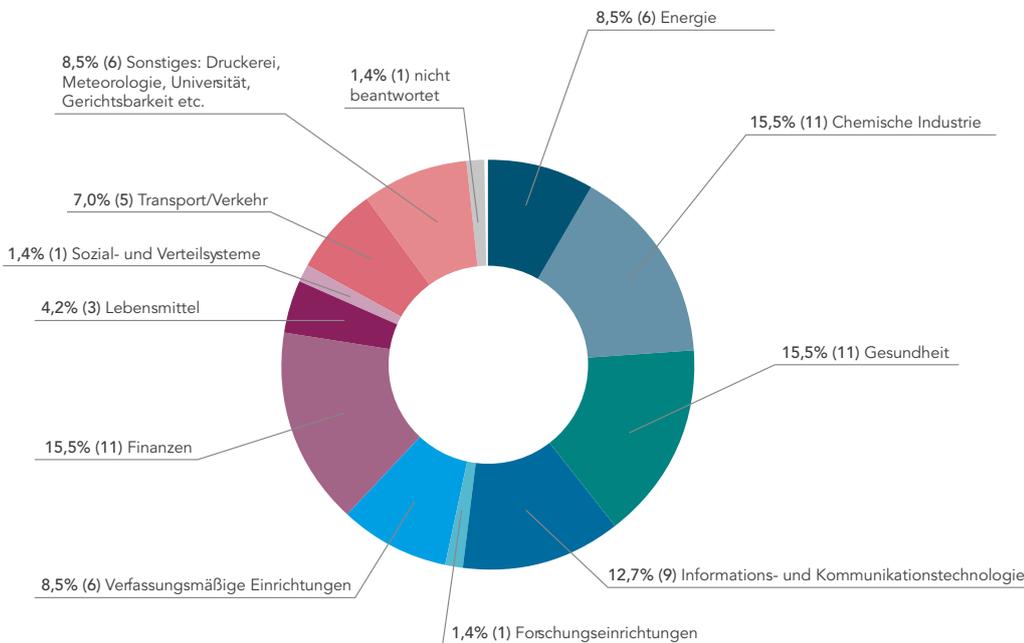


Abbildung 1: Gliederung der Antworten nach Branchen

### Verteilung nach Größe der Organisation

Die Verteilung der TeilnehmerInnen nach Anzahl der MitarbeiterInnen spiegelt die Verteilung in den Unternehmen bzw. Organisationen wider.

Mehr als die Hälfte (50,7 %) der Antwortenden gaben an, aus einem Unternehmen bzw. einer Organisation mit mehr als 1.000 MitarbeiterInnen zu stammen. Bei 31,0 % sind 250-1.000 MitarbeiterInnen beschäftigt, bei 18,3 % 50-249 MitarbeiterInnen.

Innerhalb der kritischen Infrastruktur in Österreich gibt es derzeit keine Organisation mit weniger MitarbeiterInnen.

Wie viele MitarbeiterInnen sind in Ihrem Unternehmen bzw. Ihrer Organisation beschäftigt?

N=71

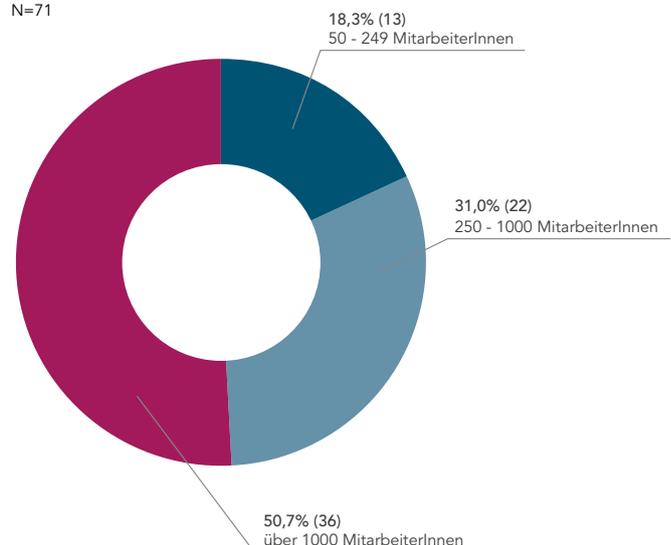


Abbildung 2: Größenverteilung der Unternehmen/Organisationen der Antwortenden

### Tätigkeitsbereich der Antwortenden nach Unternehmen bzw. Organisationen

Betrachtet man den geographischen Tätigkeitsbereich der Unternehmen bzw. Organisationen der Teilnehmenden, ergibt sich folgende Verteilung:

Der überwiegende Teil der Antwortenden (60,6 %) stammt aus Unternehmen bzw. Organisationen, die international tätig sind. Bei weiteren 22,5 % erstreckt sich der Tätigkeitsbereich auf ganz Österreich, bei den restlichen 16,9 % auf Teile Österreichs.

### Organisatorische Zuordnung

Die Frage nach der persönlichen organisatorischen Zuordnung beantworteten die Sicherheitsverantwortlichen unterschiedlich.

Etwas mehr als ein Drittel (35,2 %) der Sicherheitsverantwortlichen sind als Stabsstelle organisiert, etwa ein Viertel ist einer Stabsabteilung zugeordnet (25,4 %) oder Teil des Top Managements (23,9%).

Die verbleibenden zehn Antworten gaben sonstige Zuordnungen an, etwa die Tätigkeit als CIO oder in der IT, im Facility Management, als Leitungsfunktion der Instandhaltung etc. Diese Unterschiede ergeben sich aus der Kombination von unterschiedlichen Organisationsformen und unterschiedlicher Trägerschaft (öffentlich oder privat), Unternehmensgrößen und Branchenerfordernissen bzw. möglichen Bedrohungen. Wie die tatsächliche Tätigkeit ausgestaltet ist, welche Aufgaben und Kompetenzen damit verbunden sind und wie hoch der Stellenwert von Sicherheit im Unternehmen bzw. der Organisation ist, lässt sich daraus nicht ableiten. Formell sind die Gestaltungsspielräume am größten, wenn die/der Sicherheitsverantwortliche selbst Teil des Managements ist.

### Zeitliche Ressourcen für die Aufgaben als Sicherheitsverantwortliche/r

Höchst unterschiedlich ist auch das Ausmaß an Stunden verteilt, die den Sicherheitsverantwortlichen pro Woche zur Verfügung stehen. Dies ergibt sich auch hier wiederum aus unterschiedlichen Organisationsformen, Branchen etc.

Die Antworten zeigen eine U-Kurve mit den höchsten Werten an den Rändern:

Bei einem Großteil der Antwortenden ist Sicherheit eine Teilzeitaufgabe. (Mehr als ein Drittel sind unter zehn Stunden pro Woche damit befasst). Gleich viele Antworten entfielen andererseits auf über 31 Stunden pro Woche.

Das Mittelfeld dazwischen ist entsprechend schwächer ausgeprägt.

Vergleichsweise hoch mit 9,9 % ist hier außerdem der Anteil jener Antwortenden, die keine Angabe machten.

Der Tätigkeitsbereich des Unternehmens bzw. der Organisation ist ...  
N=71

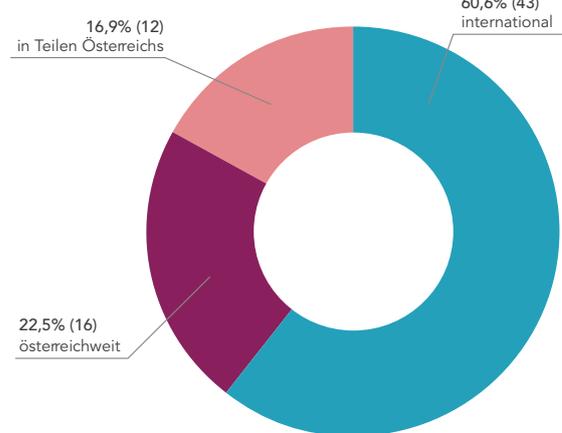


Abbildung 3: Tätigkeitsbereiche der Unternehmen/Organisationen

Wo sind Sie als „Sicherheitsverantwortliche/r“ organisatorisch zugeordnet?  
N=71

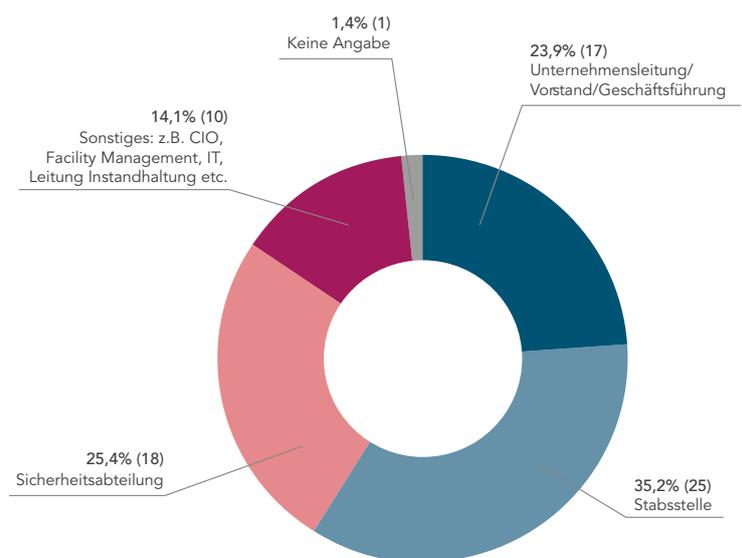


Abbildung 4: Organisatorische Zuordnung der Befragten

Wie viele Stunden stehen Ihnen in Ihrem Unternehmen bzw. Ihrer Organisation für die Aufgaben als Sicherheitsverantwortliche/r wöchentlich zur Verfügung?  
N=71

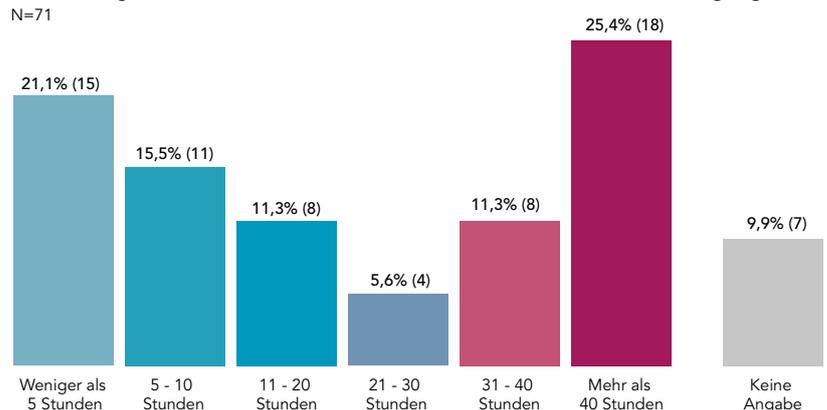


Abbildung 5:

Wöchentliche Stundenanzahl für die Tätigkeit als Sicherheitsverantwortliche/r

## ERWARTUNGEN IN BEZUG AUF EINZELNE BEDROHUNGEN

In Bezug auf die allgemeine Bedrohungslage bis ins Jahr 2022 wird allgemein und überwiegend mit einem Anstieg gerechnet.

Die Bedrohung durch IT-Angriffe wird weiter ansteigen, da sind sich alle Antwortenden einig. 92,8 % erwarten das auch für Social Engineering (das meist eine Begleit-handlung für andere Bedrohungen darstellt); 5,5 % sehen diese Bedrohung als für sich nicht relevant an. Weltanschaulich und politisch motivierter Extremismus/ Terrorismus liegt mit 74,2 % an dritter Stelle, wobei hier

nahezu ein Viertel (22,6 %) von keiner Relevanz für ihre Organisation bzw. ihr Unternehmen ausgeht.

Bei Spionage gehen zwei Drittel von einer steigenden Bedrohungslage bis 2022 aus. Gewalthandlungen und Sabotage liegen minimal dahinter.

Selbst bei Sabotage geht noch nahezu die Hälfte davon aus, dass diese Bedrohung ansteigen wird, wobei mehr als ein Drittel angibt, dass diese Bedrohung für sie nicht relevant ist.

Aus Gründen der Übersichtlichkeit wurden hier fehlende Angaben („keine Antwort“) nicht dargestellt.

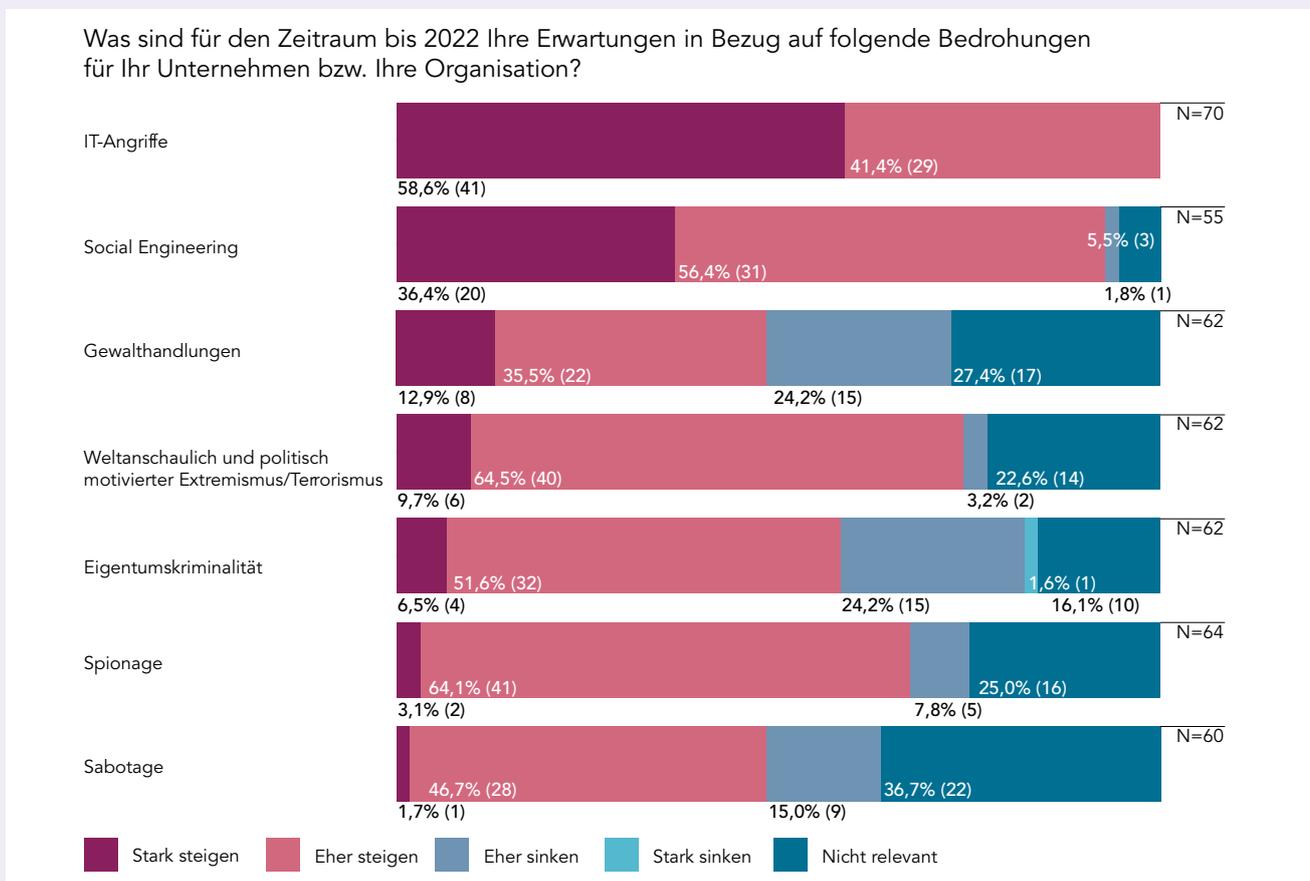


Abbildung 6: Erwartung künftiger Bedrohungen durch die Sicherheitsverantwortlichen

## HALTUNG ZU VERBINDLICHEN AUSBILDUNGSSTANDARDS FÜR SICHERHEITSDIENSTLEISTERINNEN

Etwa vier von fünf der befragten Sicherheitsverantwortlichen tritt für verbindliche Ausbildungsstandards für SicherheitsdienstleisterInnen in Österreich ein. Dem gegenüber steht eine einzige Meldung, die dies nicht be-

fürwortet. Der Rest äußerte sich indifferent: 11,3 % gaben hier die Option „ist mir egal“ an, 5,6 % machten keine Angabe.

Würden Sie verbindliche Ausbildungsstandards für Sicherheitsdienstleister in Österreich befürworten?

N=71

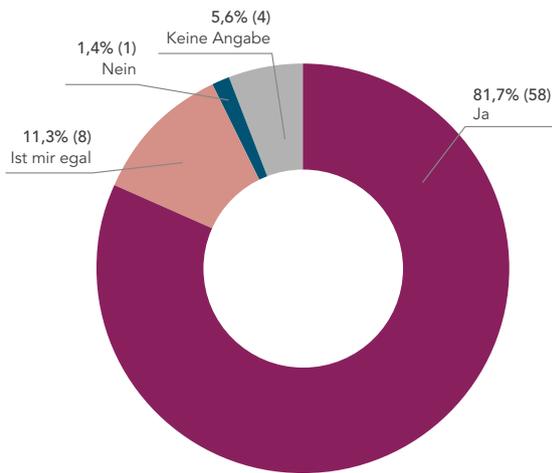


Abbildung 7:  
Haltung zu verbindlichen Mindeststandards in der Ausbildung der Beschäftigten der SicherheitsdienstleisterInnen



## SICHERHEITSORGANISATION IM UNTERNEHMEN

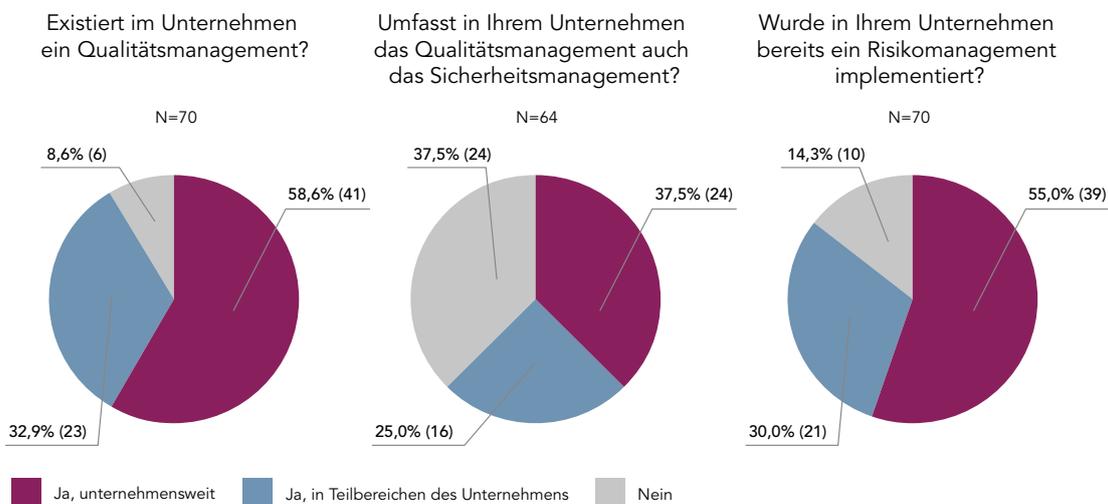


Abbildung 8: Verbreitung und Umfang von Qualitäts-, Sicherheits- und Risikomanagement

### Vorhandensein von Qualitäts- und Risikomanagement

Beim Großteil der Befragten sind heute Qualitäts- und Risikomanagement mittlerweile unternehmensweit etabliert; oft ist auch das Sicherheitsmanagement Teil davon. Bezüglich Qualitätsmanagement kam die Definition der ÖNORM EN ISO 9000:2015 zur Anwendung: „Qualitätsmanagement kann das Festlegen der Qualitätspolitiken und der Qualitätsziele sowie Prozesse für das Erreichen dieser Qualitätsziele durch Qualitätsplanung, Qualitätssicherung, Qualitätssteuerung und Qualitätsverbesserung umfassen.“

Für diese Umfrage wurde der Begriff „Sicherheit“ definiert; die Definition wurde den Befragten zu Beginn mitgeteilt. Sicherheit umfasste demnach „physische Sicherheit, Datensicherheit etc. (also Security)“; ausdrücklich nicht umfasst waren dabei die gesetzlich geregelten Themen Arbeitssicherheit, Brandschutz, Gefahrstoffe, Schutz vor Naturkatastrophen etc. (Safety).

Nach dem Verständnis der Umfrage umfasst Risikomanagement laut ONR 49000:2014 „Prozesse und Verhaltensweisen, die darauf ausgerichtet sind, eine Organisation bezüglich Risiken zu steuern“.

In mehr als 9 von 10 Unternehmen bzw. Organisationen, aus denen die Antwortenden kommen, ist bereits Qualitätsmanagement implementiert, überwiegend unternehmensweit, teilweise auch nur in Teilbereichen.

Mehr als die Hälfte der Antworten entfielen darauf, dass Sicherheitsmanagement vom Qualitätsmanagement umfasst ist, zumindest in Teilbereichen der Organisation. Risikomanagement ist bei 85,7 % der Antwortenden bereits implementiert, bei 55 % sogar auf Ebene der gesamten Organisation.

### Verbreitung und Implementierung bestimmter Normen und Standards

Im Bereich Qualitäts-, Risiko- und Sicherheitsmanagement existiert eine Reihe von Normen und Standards. In einer Übersicht wurde abgefragt, welche davon wie stark verbreitet sind.

Mehr als die Hälfte der Antwortenden ist in Unternehmen bzw. Organisationen tätig, die Qualitätsmanagement nach ISO 9001 implementiert haben bzw. danach zertifiziert sind.

Ebenfalls noch stark verbreitet sind die Normenfamilien für Informationsmanagement (ÖVE/ÖNORM EN ISO / IEC 27000) und Risikomanagement (zusammengefasst ÖNORM ISO 31000 bzw. ONR 49000 Serie).

Alle weiteren abgefragten Normen und Standards fallen dagegen stark ab; wobei bei allen ein Anteil identifiziert werden kann, bei dem die Umsetzung in Planung oder bereits in Arbeit ist.

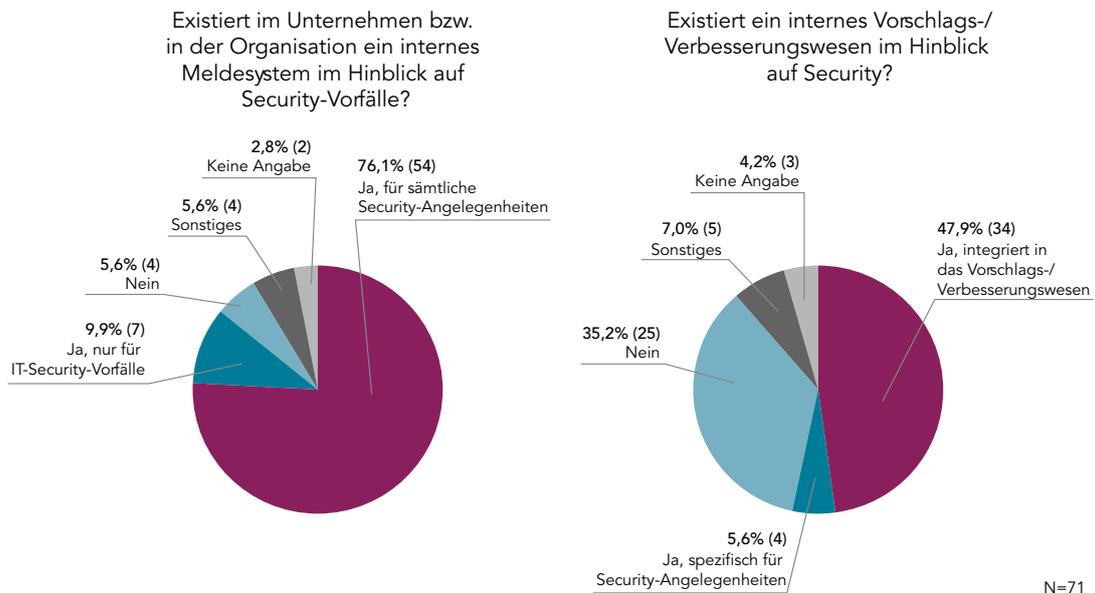


Abbildung 9: Meldesysteme und Vorschlags- bzw. Verbesserungswesen in den Unternehmen/Organisationen der Befragten

### Meldesystem und Vorschlagswesen

Meldesysteme sind weiter verbreitet als entsprechende Vorschlags- bzw. Verbesserungswesen; meist umfassen sie sämtliche Security-Angelegenheiten. Ein Vorschlags- bzw. Verbesserungswesen kann im Rahmen eines formalisierten Qualitätsmanagements oder unabhängig davon eingerichtet werden.

Mehr als drei Viertel (76,1 %) der Antwortenden gaben an, dass in ihrer Organisation ein allgemeines Meldesystem für Security Vorfälle existiert; weitere 9,9 % gaben an, dass ein solches für IT-Security-Vorfälle zur Verfügung steht. In manchen Branchen (z.B. Finanzwirtschaft) ist ein Meldewesen für bestimmte Vorfälle gesetzlich verpflichtend vorgesehen, auch die Umsetzung der NIS-Richtlinie wird BetreiberInnen wesentlicher Dienste besonderen

Meldepflichten unterwerfen. Nahezu die Hälfte der Sicherheitsverantwortlichen (47,9 %) hat in ihrer Organisation bzw. in ihrem Unternehmen ein Vorschlags-/Verbesserungswesen, das auch Security-Themen umfasst. In vier weiteren Fällen wurde ein solches spezifisch für Sicherheitsangelegenheiten eingeführt.

Anmerkung: Mit der NIS-Richtlinie, die am 8. August 2016 in Kraft getreten ist, soll EU-weit ein hohes Sicherheitsniveau von Netz- und Informationssystemen erreicht werden. Vor diesem Hintergrund soll die Zusammenarbeit zwischen den Mitgliedstaaten in strategischer und operationeller Hinsicht gestärkt sowie bestimmte wichtige (private und öffentliche) AnbieterInnen zu angemessenen Sicherheitsmaßnahmen und zur Meldung erheblicher Störfälle verpflichtet werden.<sup>1</sup>

<sup>1</sup> Weiterführende Informationen dazu finden sich auf <https://www.digitales.oesterreich.gv.at/eu-richtlinie-zur-netz-und-informationssicherheit> [24.11.2018]

## ZUSAMMENARBEIT MIT EXTERNEN DIENSTLEISTERINNEN – BERATUNG

Eine Reihe externer Beratungseinrichtungen steht für Unternehmen bzw. Organisationen der kritischen Infrastruktur zur Verfügung. Um einen Überblick zu bekommen, wurde zu Beginn eine Reihe „typischer“ Möglichkeiten abgefragt, bei denen potenziell Beratung möglich ist.

Die Antworten sagen nur etwas über die Häufigkeit, aber nichts über die Qualität/Intensität, den Anlass oder den möglichen Erfolg der jeweiligen fachlichen Beratung aus. Vorab anzumerken ist, dass Institutionen wie die Wirtschaftskammer oder Branchennetzwerke überwiegend für deren jeweilige Mitglieder relevant sind und z.B. nicht alle Unternehmen/Organisationen in der Wirtschaftskammer organisiert sind. Das BMI und das Bundesamt (BVT) sowie die Landesämter für Verfassungsschutz und Terrorismusbekämpfung (LVT) wurden von nahezu allen Befragten (90,9 %) seit 2015 zumindest ein Mal wegen fachlicher Beratung in Sicherheitsfragen in Anspruch genommen. Ähnlich hoch ist der Wert bei IT-DienstleisterInnen, wobei bei diesen die monatliche Beratung noch stärker ausgeprägt ist. Auch Beratung durch Sicherheitsgewerbe/Bewachungsunter-

nehmen wird stark nachgefragt, bei monatlicher Beratung ist der Wert mit 14,7 % der höchste. Etwas geringer ausgeprägt sind die Werte für Branchennetzwerke.

UnternehmensberaterInnen/SicherheitsberaterInnen und der kriminalpolizeiliche Beratungsdienst rangieren im Mittelfeld; Beratung wird hier überwiegend bei konkreten Anlassfällen in Anspruch genommen.

Vergleichsweise geringer ausgeprägt ist die Inanspruchnahme der Dienstleistungen von Hochschulen und Forschungseinrichtungen, Versicherungen/VersicherungsmaklerInnen, BerufsdetektivInnen und der Wirtschaftskammer.

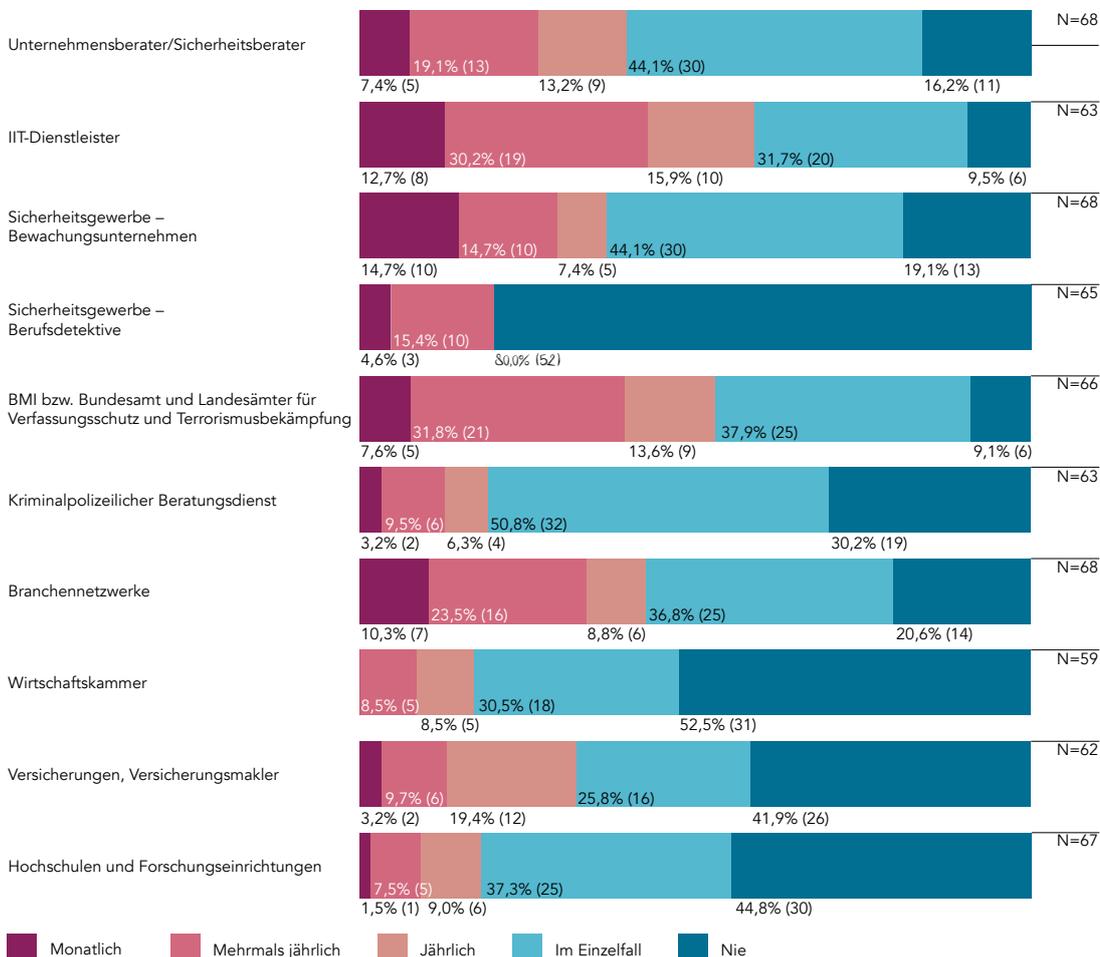
### Zufriedenheit mit externer Beratung

Generell zeigt sich bei den Befragten eine hohe Zufriedenheit mit der erhaltenen Beratungsleistung.

Spitzenreiter sind das Bundesministerium für Inneres bzw. BVT und LVTs, der kriminalpolizeiliche Beratungsdienst sowie Branchennetzwerke.

Bei der Interpretation im Detail ist zu bedenken, dass manche der genannten Angebote kostenlos, andere kos-

Wie oft haben Sie von einem der folgenden Anbieter in Österreich im Zeitraum seit 2015 fachliche Beratung in Sicherheitsfragen in Anspruch genommen?



Außerdem genannt wurden u.a.: Bundeskanzleramt, Bundesministerium für Landesverteidigung, Heeresnachrichtenamt, Heeresabwehramt, Landeskriminalamt, Cyber Security Platform, cert.at

Abbildung 10: Frequenz der Inanspruchnahme externer Organisationen für Beratungen

Wie zufrieden waren Sie mit der externen Beratung?

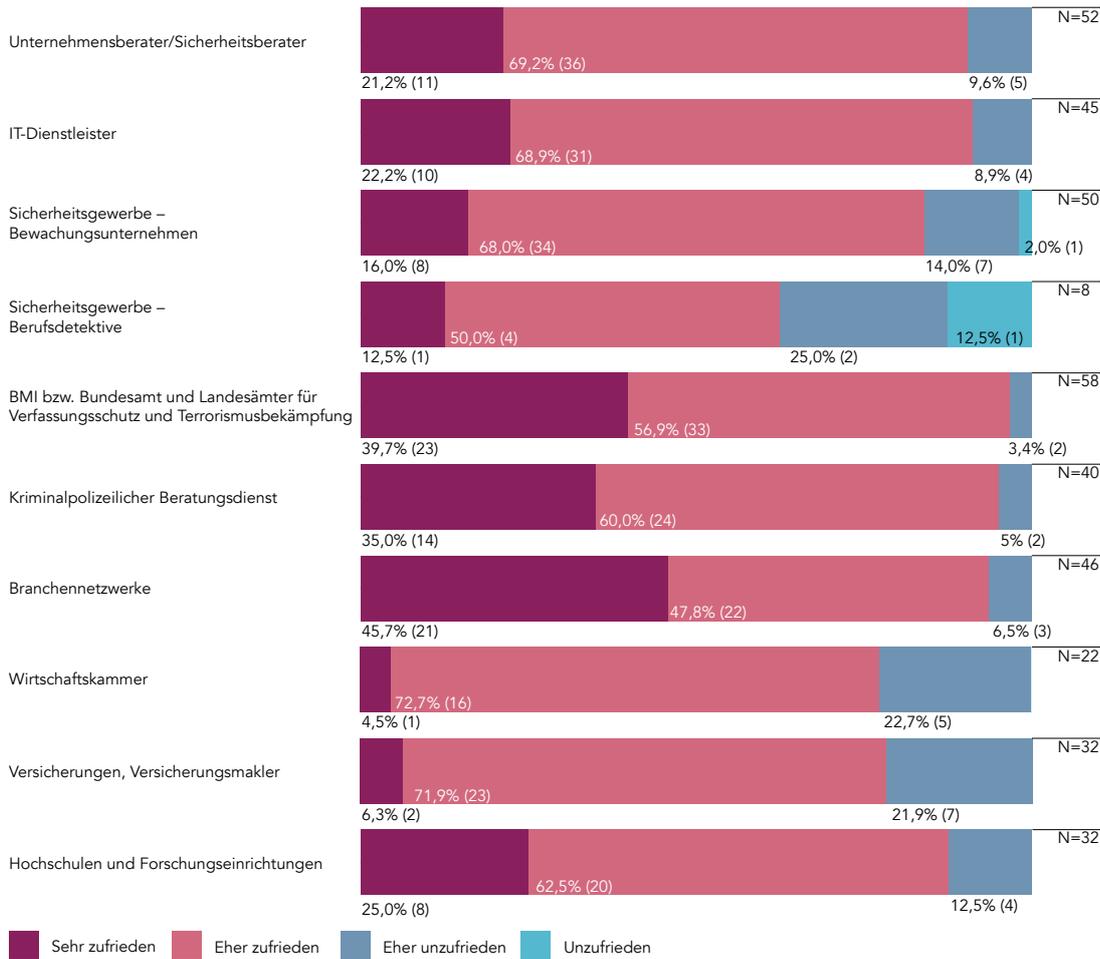


Abbildung 11: Zufriedenheit der Befragten mit der in Anspruch genommenen Beratung

tenpflichtig sind. Daher ist ein direkter Vergleich oft nicht sinnvoll. Außerdem ergibt sich eine Einschränkung der Interpretierbarkeit durch die große Bandbreite der Anzahl der Antworten (zwischen 8 und 58).

**Gründe für die Inanspruchnahme externer Beratung**

Externe Expertise ist aus unterschiedlichen Gründen gefragt. Meist sind mehrere Gründe für die Befragten ausschlaggebend.

Prävention ist der wichtigste Grund, Beratung in Anspruch zu nehmen, wie dahingehende Antworten durch drei von

vier der Befragten zeigen. Darauf folgt eine Gruppe mit unterschiedlichen Gründen – konkrete Anlassfälle, rechtliche Auflagen, spezifischer Beratungsbedarf –, aufgrund derer die Beratung konkret geboten war. Jeweils etwa sechs von zehn Kontakten, die den Fragebogen ausgefüllt haben, gaben diese Optionen an.

Der Bedarf an unabhängiger externer Expertise und das Fehlen eigener Ressourcen sind für jeweils vier von zehn der Antwortenden Gründe für Beratung.

Interne Auflagen waren bei etwa einem Drittel der Antwortenden Auslöser für die Beauftragung externer Dienstleistungen.

Welche der folgenden Gründe haben Sie dazu veranlasst diese Beratungsdienstleistungen in Anspruch zu nehmen?

N=71; Mehrfachnennungen möglich  
 Weitere genannte Gründe: Info durch Polizei, Umsetzung NIS-Richtlinie

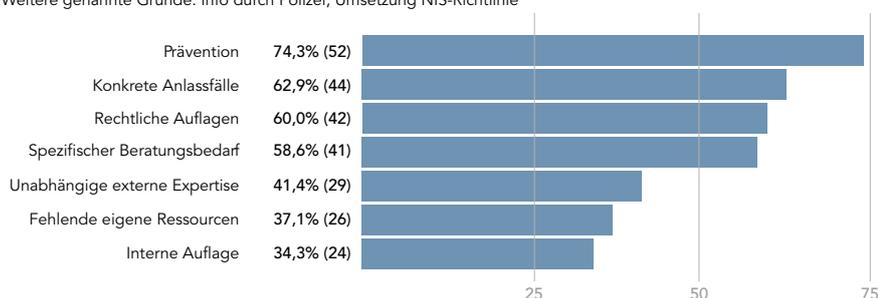


Abbildung 12: Gründe für externe Beratung

**Geplante externe fachliche Beratung**

Der Beratungsbedarf in nächster Zeit hält weiter an; dabei überwiegen meist mittelfristige Anforderungen.

Bei der bereits geplanten externen fachlichen Beratung im Zeitraum der nächsten 36 Monate bildet das Bundesministerium für Inneres bzw. BVT und LVTs gemeinsam mit IT-Beratungsunternehmen und Unternehmens-/Sicherheitsberatung die Spitzengruppe. Bemerkenswert ist weiters, dass jeweils rund jede/r fünfte

Antwortende plant, die Expertise von folgenden Stellen in den nächsten zwölf Monaten in Anspruch zu nehmen: Hochschulen und Forschungseinrichtungen, UnternehmensberaterInnen/SicherheitsberaterInnen, BMI/BVT, Versicherungen/VersicherungsmaklerInnen, aber wiederum auch Sicherheitsgewerbe/Bewachungsunternehmen.

Auffallend gering ausgeprägt ist der Wert für die nächsten zwölf Monate geplante Beratung nur im Bereich der Berufsdetektiv/e/innen.

Planen Sie von einem (oder mehreren) der folgenden Anbieter künftig fachliche Beratung in Sicherheitsfragen in Anspruch zu nehmen?

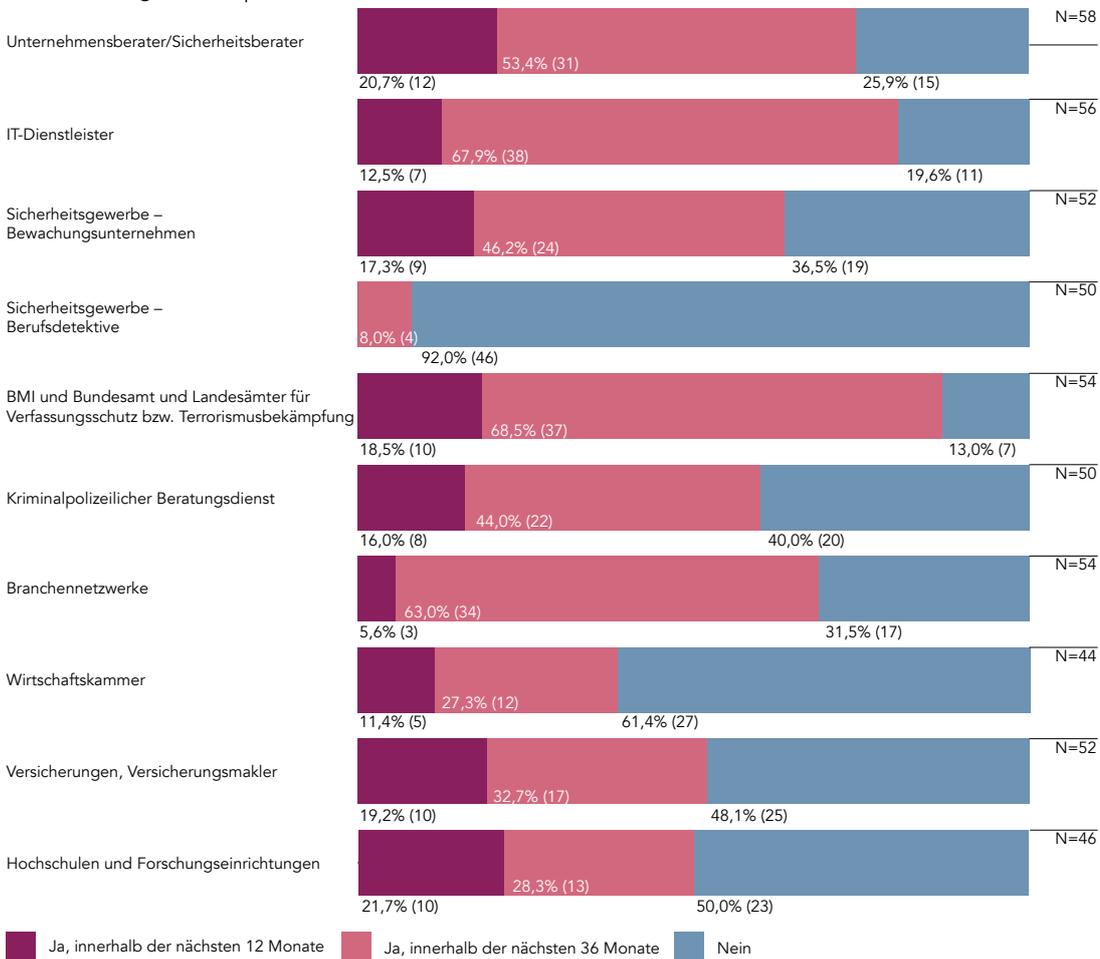


Abbildung 13: Zeithorizont geplanter künftiger Beratung

## OPERATIVE SICHERHEITSAUFGABEN INTERN: ORGANISATION UND QUALIFIKATION

Verfügt Ihr Unternehmen bzw. Ihre Organisation über folgende interne MitarbeiterInnen für operative Sicherheit?

N=71; Mehrfachnennungen möglich; Als weitere Tätigkeiten wurden genannt: SIRT-Team, CERT, Sicherheitsabteilung, Überwachungswarten

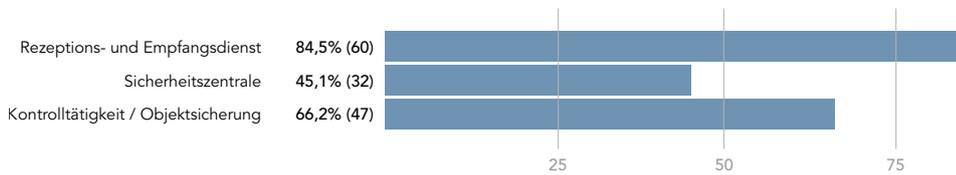


Abbildung 14: Einsatz von eigenen (internen) Beschäftigten für Sicherheitsaufgaben

### Interne MitarbeiterInnen für operative Sicherheitsaufgaben

In den Unternehmen bzw. Organisationen der Sicherheitsverantwortlichen, die den Fragebogen beantwortet haben, ist die Beschäftigung von internem Personal für operative Sicherheitsaufgaben weit verbreitet.

Am häufigsten (84,5 %) werden Rezeptions- und Empfangsdienst übernommen; in zwei Dritteln der Fälle werden Kontrolltätigkeiten und Objektsicherung durch interne Kräfte abgedeckt. Die Sicherheitszentrale wird bei 45,1 % der Antwortenden durch eigene MitarbeiterInnen besetzt. Anzumerken zu dieser Antwortoption ist, dass eine Sicherheitszentrale nicht in sämtlichen Organisationen bzw. Unternehmen der kritischen Infrastruktur etabliert ist.

Aus der Fragestellung ist nicht ablesbar, ob diese Aufgaben kombiniert von einzelnen Beschäftigten abgedeckt werden.

### Verteilung zwischen interner und externer Ausbildung

Internes Sicherheitspersonal wird bei den Befragten – bis auf einzelne Ausnahmefälle – besonders geschult und ausgebildet.

Die Überschneidung bei den Antwortoptionen legt nahe, dass in zahlreichen Fällen interne Ausbildungsinhalte mit den Angeboten externer Bildungseinrichtungen kombiniert werden.

Hohe Werte mit über zwei Drittel der Antworten bei der externen Ausbildung verzeichnen die Sicherheitszentrale und die Kontrolltätigkeit/Objektsicherung.

Wie sich durch die geringere Anzahl der Antwortenden zeigt, sind Sicherheitszentralen in den Unternehmen bzw. Organisationen der kritischen Infrastruktur weniger verbreitet.

### Inhalte und Ausmaß der Ausbildung für die jeweiligen Tätigkeiten

Die meisten der abgefragten Ausbildungsinhalte (rechtliche Rahmenbedingungen, aufgabenspezifisches Verhaltenstraining, Melde- und Berichtswesen, Psychologie/Konfliktmanagement, Zusammenarbeit mit Behörden und externen Stellen, Bedienung von Sicherheitstechnik/Gefahrenmeldeanlagen, Erste Hilfe und Brandschutz) werden in bis zu zehn Stunden vermittelt, wobei nur für wenige Fachgebiete derzeit mehr als 30 Stunden angegeben werden.

In zahlreichen Ausbildungen für Rezeptions- und Empfangsdienste sind die Themen Psychologie/Konfliktmanagement, die Zusammenarbeit mit Behörden und externen Stellen sowie rechtliche Rahmenbedingungen gar nicht umfasst.

Sicherheitszentralen sind weitaus weniger häufig verbreitet. Bei der Ausbildung der dort tätigen MitarbeiterInnen zeigen sich einzig dort deutliche Abweichungen in Bezug auf die oben erläuterten Antworten: Die Ausbildung der dort eingesetzten MitarbeiterInnen umfasst nahezu immer sämtliche angegebenen Optionen. Eine einzige Ausnahme stellt Psychologie/Konfliktmanagement dar. Aufgabenbedingt ist von der Stundenanzahl der Aspekt „Bedienung von Sicherheitstechnik/Gefahrenmeldeanlagen“ her besonders stark ausgeprägt.

Wie erfolgt die Ausbildung dieser MitarbeiterInnen für folgende Tätigkeiten?

Mehrfachnennungen möglich

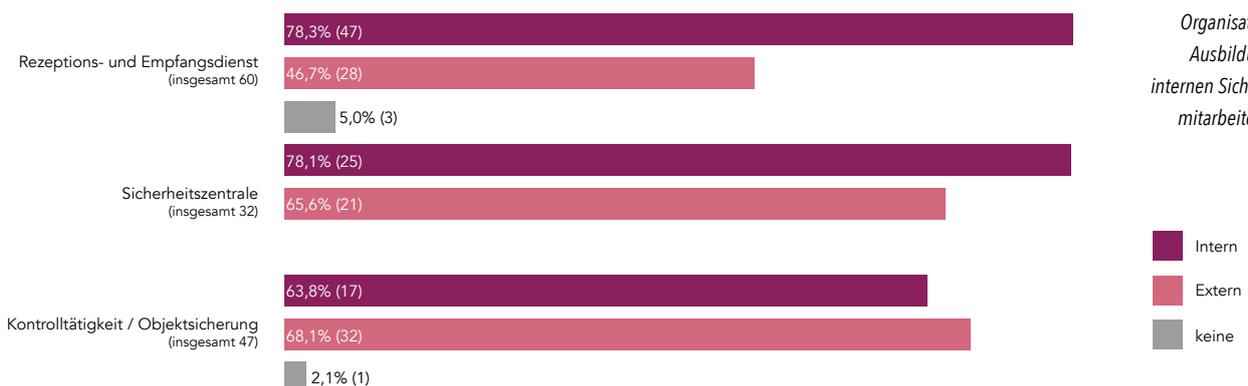


Abbildung 15: Organisation der Ausbildung der internen SicherheitsmitarbeiterInnen

## OPERATIVE SICHERHEIT: ZUSAMMENARBEIT MIT EXTERNEN DIENSTLEISTERINNEN

Setzt Ihr Unternehmen bzw. Ihre Organisation externe Bewachungsunternehmen ein?

N=71

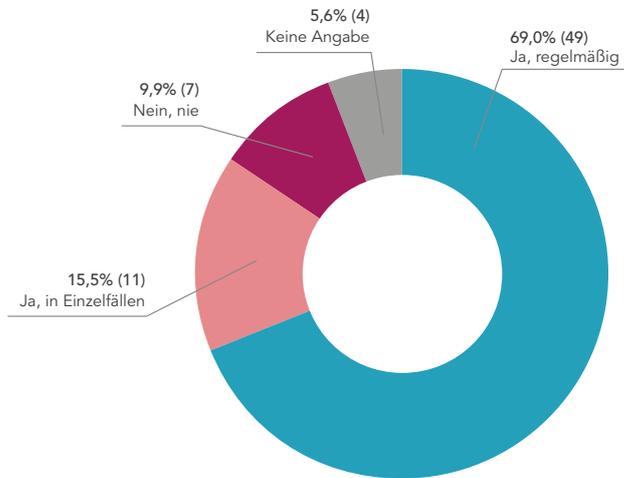


Abbildung 16:  
Verbreitung des Einsatzes  
externer Bewachungs-  
unternehmen

### Beauftragung von Bewachungsunternehmen

Externe Bewachungsunternehmen werden vom Großteil der Befragten eingesetzt.

Fünf von sechs der befragten Sicherheitsverantwortlichen – insgesamt 84,5 % – gaben an, dass in ihrem Unternehmen bzw. ihrer Organisation externe Bewachungsunternehmen eingesetzt werden, bei 69 % sogar regelmäßig. Nur bei knapp einem Zehntel ist das nie der Fall.

### Aufgaben beauftragter Bewachungsunternehmen

Die Aufgaben, die von Beschäftigten externer Bewachungsunternehmen abgedeckt werden können, sind vielfältig. Die hier in der Umfrage verwendeten Bezeichnungen entsprechen den im Kollektivvertrag für das Sicherheitsgewerbe angegebenen Verwendungsgруппen.<sup>2</sup> Bei 88,3 % der Sicherheitsverantwortlichen, die geantwortet haben, werden externe Bewachungsunternehmen mit Wachdiensten beauftragt, in 63,3 % der Fälle mit Service- und Sicherheitsdiensten.

Zum Wachdienst zählen beispielsweise Ein- und Ausweisung von Fahrzeugen, Auskunftserteilung und Telefondienst, Überwachung und Bedienung von Kontrollanlagen jeglicher Art, Kontrollgänge, Kontrolle aller Zu- und

Abgänge der zu bewachenden Objekte, ob diese verschlossen bzw. vorschriftsmäßig abgesichert sind, Auf- und Absperrdienste.

Zu Service- und Sicherheitsdienst zählen etwa Beaufsichtigung der ein- und austretenden Personen in Verbindung mit etwaigen Kontrollen, Überprüfung der ein- und ausfahrenden Fahrzeuge, Ordnungsdienste, Entgegennahme und Ausfolgung von Poststücken sowie Telefondienst für zehn oder mehr Nebenstellen und Dienst in einer ständig besetzten, Hilfe leistenden Stelle (z.B. Notruf-, Fernwirk- oder Hausleitzentrale), die nicht der Einsatzführung eines Bewachungsunternehmens dient. Jeweils rund ein Drittel der Befragten haben die Aufgaben Veranstaltungssicherheitsdienst und mobilen Dienst extern beauftragt. In weniger als einem von zehn Fällen werden Sonderdienste extern vergeben, in einem Fall der Flughafensicherheitsdienst.

### Zufriedenheit mit Dienstleistungen der Bewachungsunternehmen

Bis auf wenige Ausnahmen zeigten sich die Antworten mit der Umsetzung der Dienstleistungen sehr zufrieden oder eher zufrieden.

Zu beachten ist die große Streuung der Anzahl der ausgewerteten Antworten – zwischen 1 und 52.

Welche Aufgaben sind von der Beauftragung umfasst?

N=71

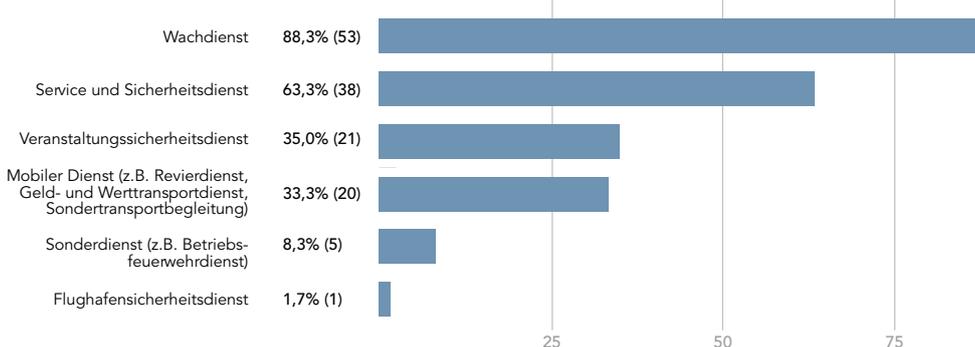


Abbildung 17:  
Aufgaben, die von  
Beschäftigten von  
Bewachungsunternehmen  
in den Unternehmen/  
Organisationen über-  
nommen werden

<sup>2</sup> Vgl. <http://www.kollektivvertrag.at/kv/wachorgane-bewachungsgewerbe-arb/wachorgane-bewachungsgewerbe-rahmen/183641> [20.11.2018].

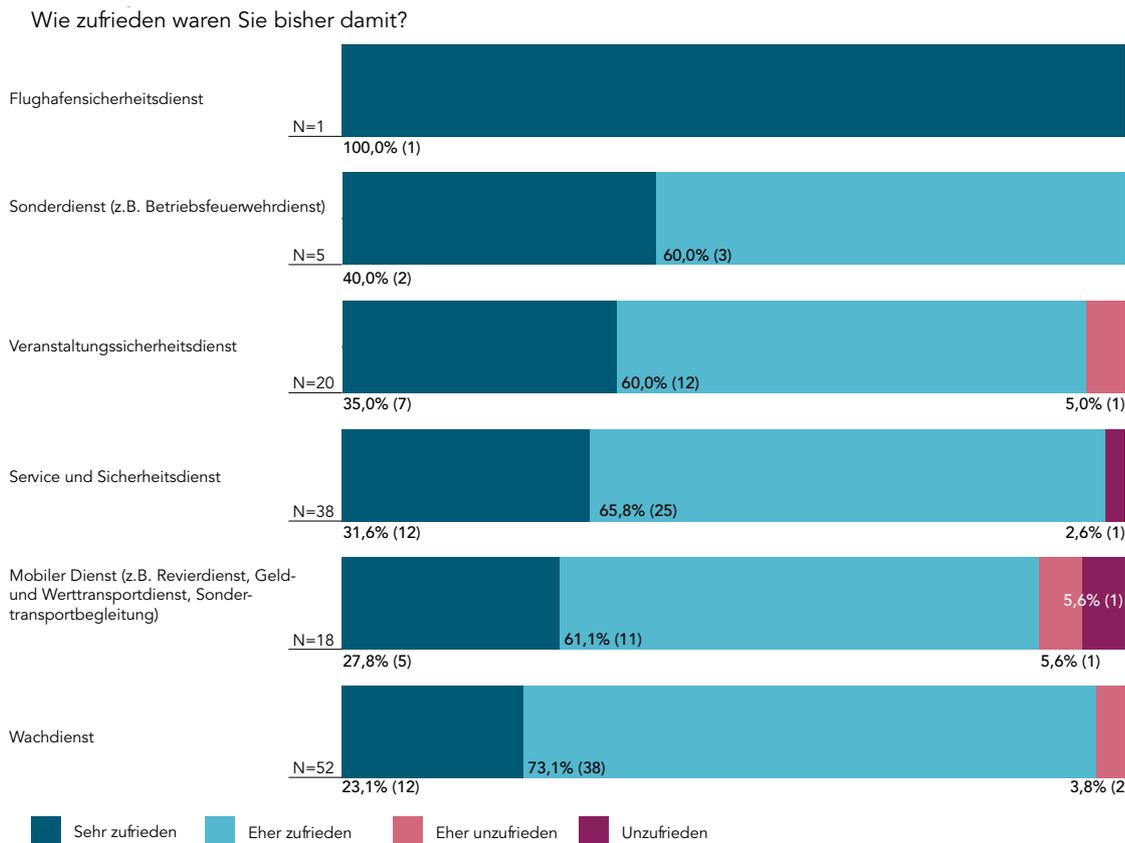


Abbildung 18: Zufriedenheit mit Dienstleistungen der Bewachungsunternehmen

### Kontinuierliche Verbesserung der Zusammenarbeit

Der Begriff der „kontinuierlichen Verbesserung“ stammt ursprünglich als Teil der Managementphilosophie Kaizen aus Japan und ist eine wichtige Säule des Qualitätsmanagements.<sup>3</sup> In ständiger Veränderung soll die Qualität der Prozesse sowie der Produkte und Dienstleistungen verbessert werden.

Die laufende Verbesserung der Zusammenarbeit erfolgt überwiegend nicht strukturiert, sondern ad hoc (70 %) oder als Reaktion nach konkreten Vorfällen (63,3 %).

In drei von zehn Fällen wird seitens des Bewachungsunternehmens allerdings aktive Beratung umgesetzt.

Wie erfolgt die kontinuierliche Verbesserung in der Zusammenarbeit mit Bewachungsunternehmen?

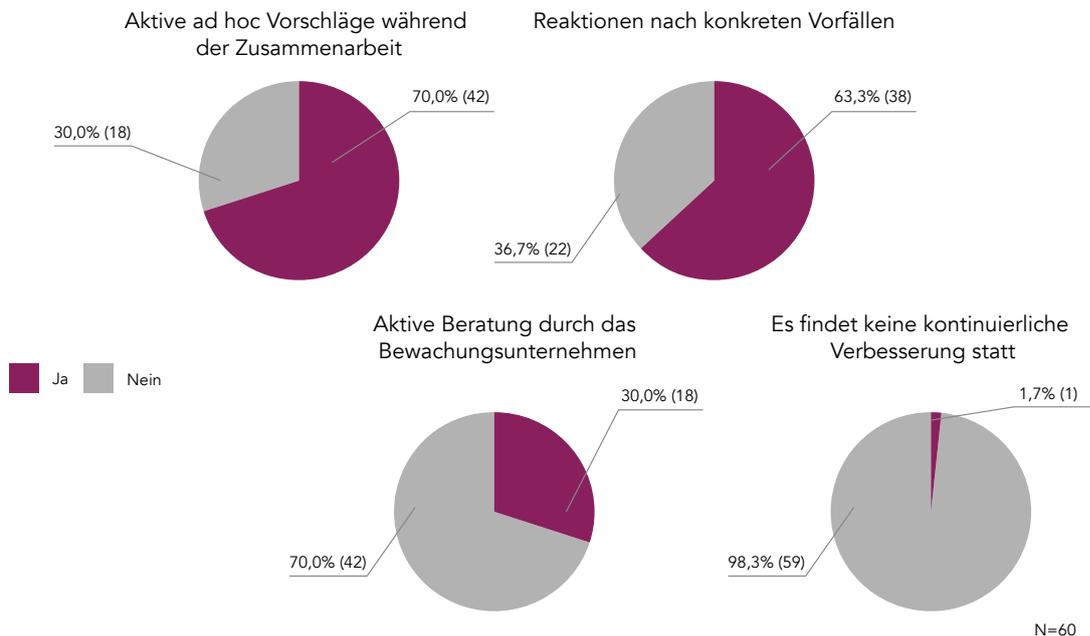


Abbildung 19: Wahrnehmung von Möglichkeiten der Verbesserung der Zusammenarbeit

<sup>3</sup> Vgl: Brockhaus, Kaizen. <http://brockhaus.at/ecs/enzy/article/kaizen> [aufgerufen am 24.11.2018]

### Qualitätskriterien bei Auswahl

Sicherheit(sdienstleistung) ist Vertrauenssache. Für die Auswahl externer SicherheitsdienstleisterInnen sind unterschiedliche Kriterien ausschlaggebend.

Die Ergebnisse zeigen deutlich, dass für die Sicherheitsverantwortlichen die nachgewiesene Ausbildung des eingesetzten Personals das wichtigste Beurteilungskriterium für die Auswahl des externen Dienstleistungsunternehmens darstellt: In mehr als neun von zehn Fällen ist diese „sehr wichtig“ bzw. „wichtig“.

Jeweils über 80 % Zustimmung erhalten die Auswahlkriterien Branchenerfahrung, Referenzen sowie Zertifizierungen. Etwas dahinter liegt das langjährige Bestehen des Unternehmens als Zeichen für Zuverlässigkeit mit rund 70 % Zustimmung in den Kategorien „sehr wichtig“ und „wichtig“. Empfehlungen bzw. Beratung durch Behörden, Beratungsunternehmen und Organisationen, die das Be-

wachungsunternehmen vorschlagen, sind überwiegend „eher wichtig“. Internationale Tätigkeit ist im Stimmungsbild der antwortenden Sicherheitsverantwortlichen eher oder ganz unwichtig.

### Vorgaben für die Qualifikation eingesetzter Personen

Die Anforderungen an die Qualifikation der eingesetzten Personen können sehr verschieden geregelt sein und über das derzeit gesetzlich vorgegebene Mindestausmaß hinausgehen.

In vier von zehn Fällen gaben die Antwortenden an, dass interne Vorgaben über die Ausschreibung festgelegt werden.

Jeweils bei 18,3 % der Fälle gibt es unternehmensweit einheitliche Vorgaben bzw. haben sich solche im Lauf der Zusammenarbeit entwickelt.

Standort- oder funktionsbezogene Vorgaben existieren in 26,7 % der Fälle.

Nach welchen Kriterien beurteilen Sie bei der Auswahl von externen Sicherheitsdienstleistern die Qualität?

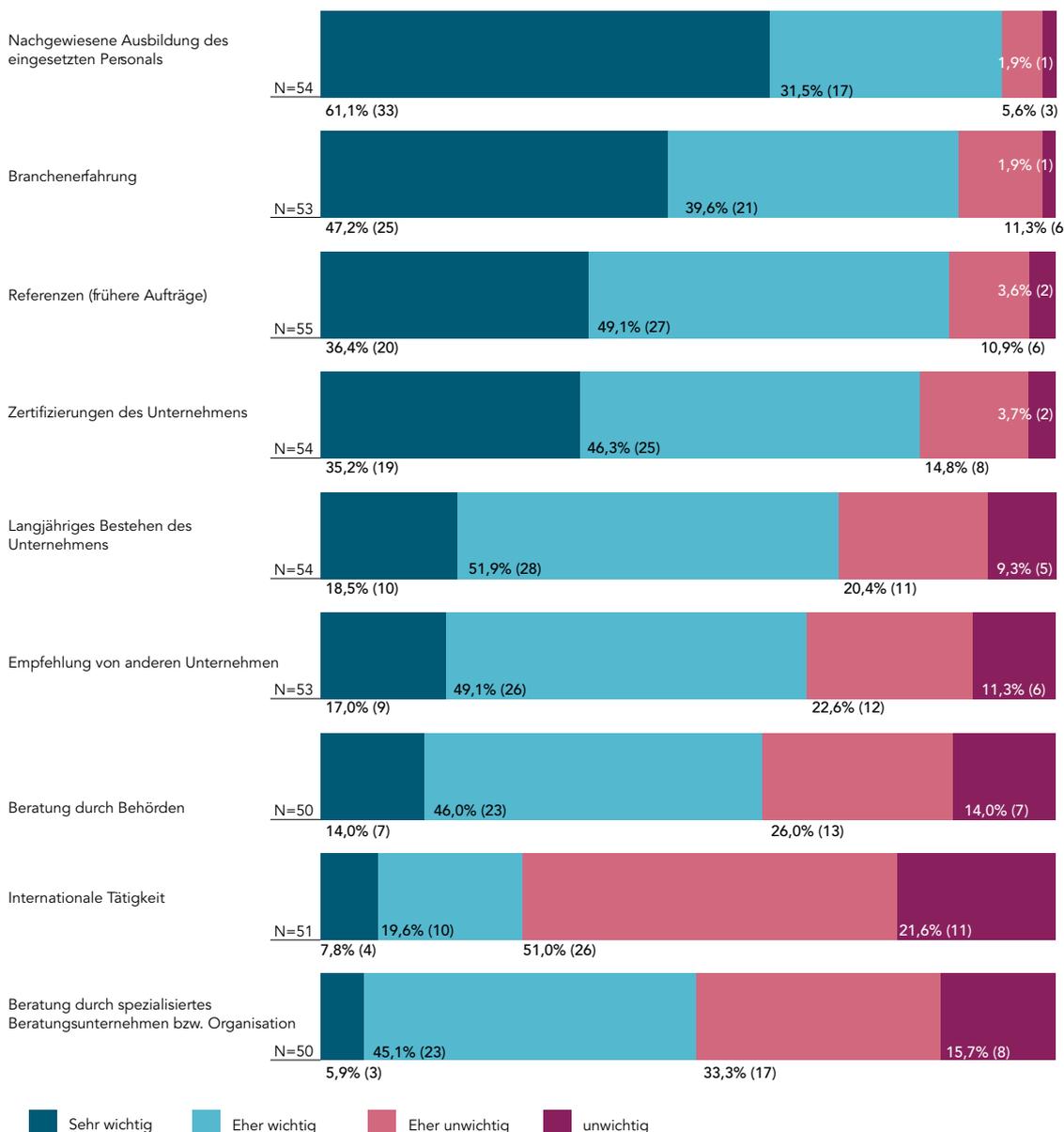


Abbildung 20: Relevanz verschiedener Kriterien für die Auswahl von AnbieterInnen von Sicherheitsdienstleistungen

In einem von sechs Fällen existieren laut den Sicherheitsverantwortlichen keine internen Vorgaben.

**Besondere Qualitätskriterien für eingesetzte Personen**

Je nach Aufgabenbereich in den Unternehmen/Organisationen sind von dem eingesetzten Personal unterschiedliche Qualitätskriterien zu erfüllen.

Bei diesen Qualitätskriterien dominieren klar Mindestanforderungen bzw. nachgewiesene Ausbildung; diese wer-

den in nahezu sieben von zehn Fällen angewendet. In vier von zehn Fällen gilt Weiterbildung als Qualitätskriterium; bei einem Drittel der Antwortenden ist mehrjährige einschlägige Berufserfahrung bedeutend.

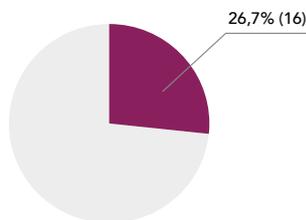
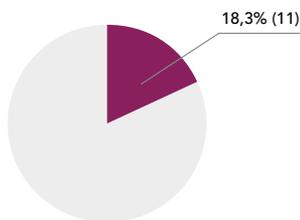
Eine besondere nachgewiesene Zuverlässigkeit ist für knapp die Hälfte der Befragten ein bedeutendes Qualitätskriterium.

Mindest- oder Höchstalter und besondere Fremdsprachenkenntnisse sind nur für rund ein Zehntel der Sicherheitsverantwortlichen relevant.

Existieren interne Vorgaben für die Qualifikation der MitarbeiterInnen externer Bewachungsunternehmen?  
N=60

Ja, unternehmensweit einheitlich

Ja, standort-/funktionsbezogen



Ja, wird über Ausschreibung festgelegt

Ja, hat sich in der Zusammenarbeit entwickelt

Nein

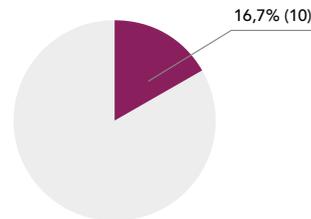
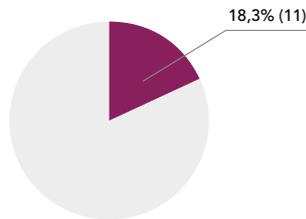
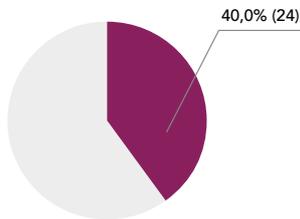


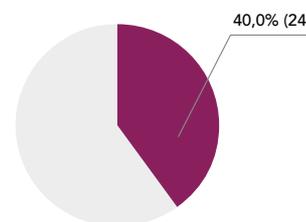
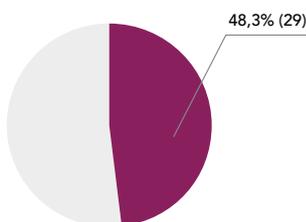
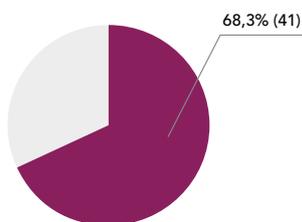
Abbildung 21: Vorhandensein und Entwicklung der Qualifikationsanforderungen der Beschäftigten von Sicherheitsdienstleistern

Welche Qualitätskriterien wenden Sie in Bezug auf das eingesetzte Personal an?  
N=71; Mehrfachnennungen möglich

Mindestanforderungen/ Nachweise für Ausbildung

Besondere Anforderungen an Zuverlässigkeit (z.B. jährliche Überprüfung der Zuverlässigkeit)

Mindestanforderungen/ Nachweise für Weiterbildung



Mehrjährige einschlägige Berufserfahrung

Mindest-/Höchstalter

Besondere Fremdsprachenkenntnisse

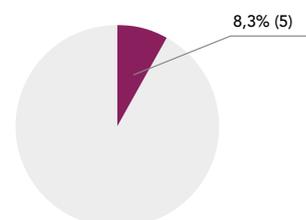
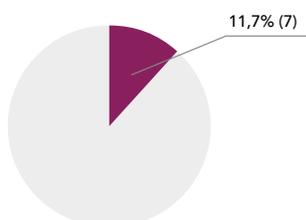
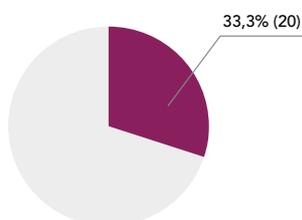
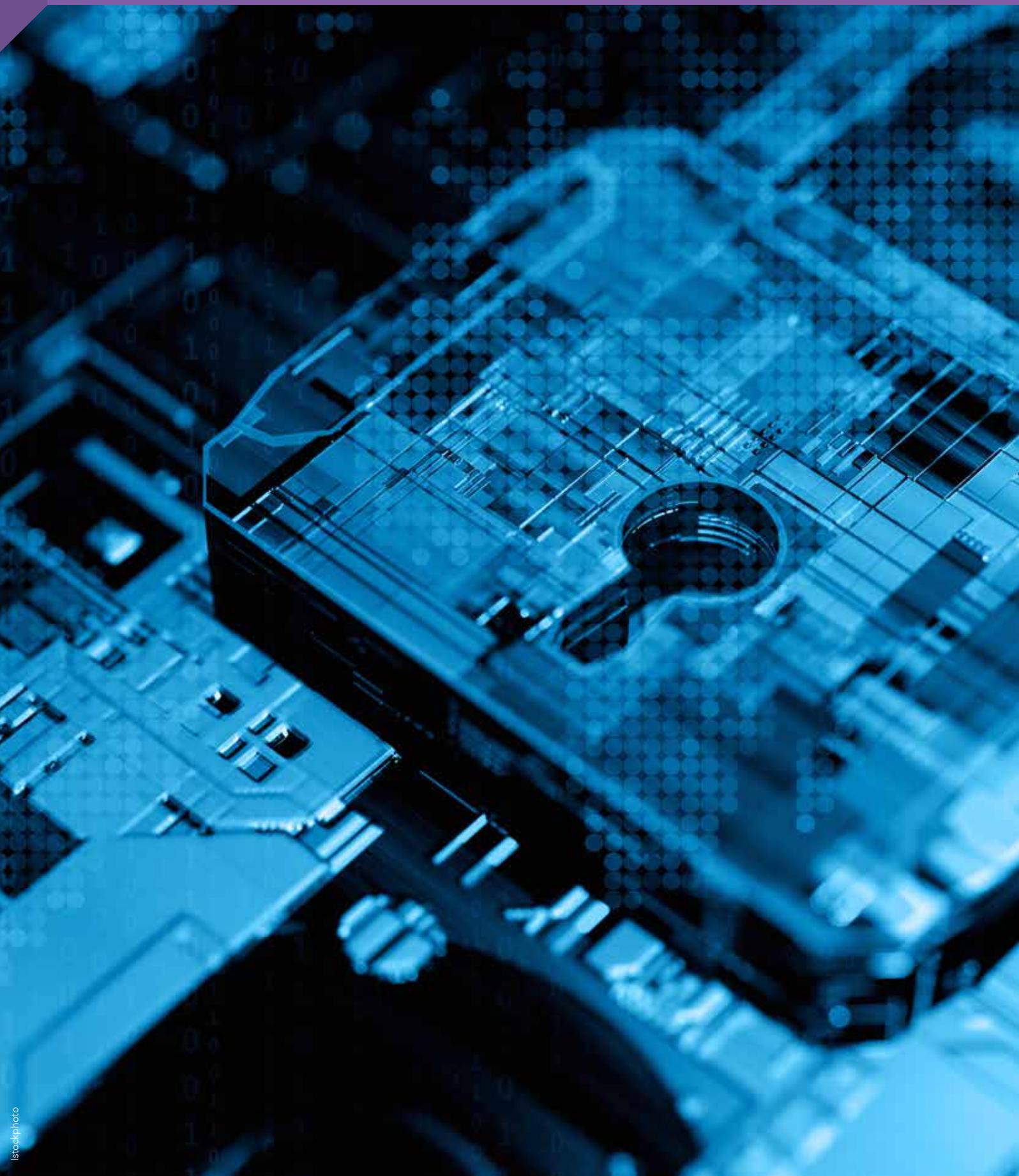


Abbildung 22: Anwendung von Qualitätskriterien auf das eingesetzte Personal

# EMPFEHLUNGEN



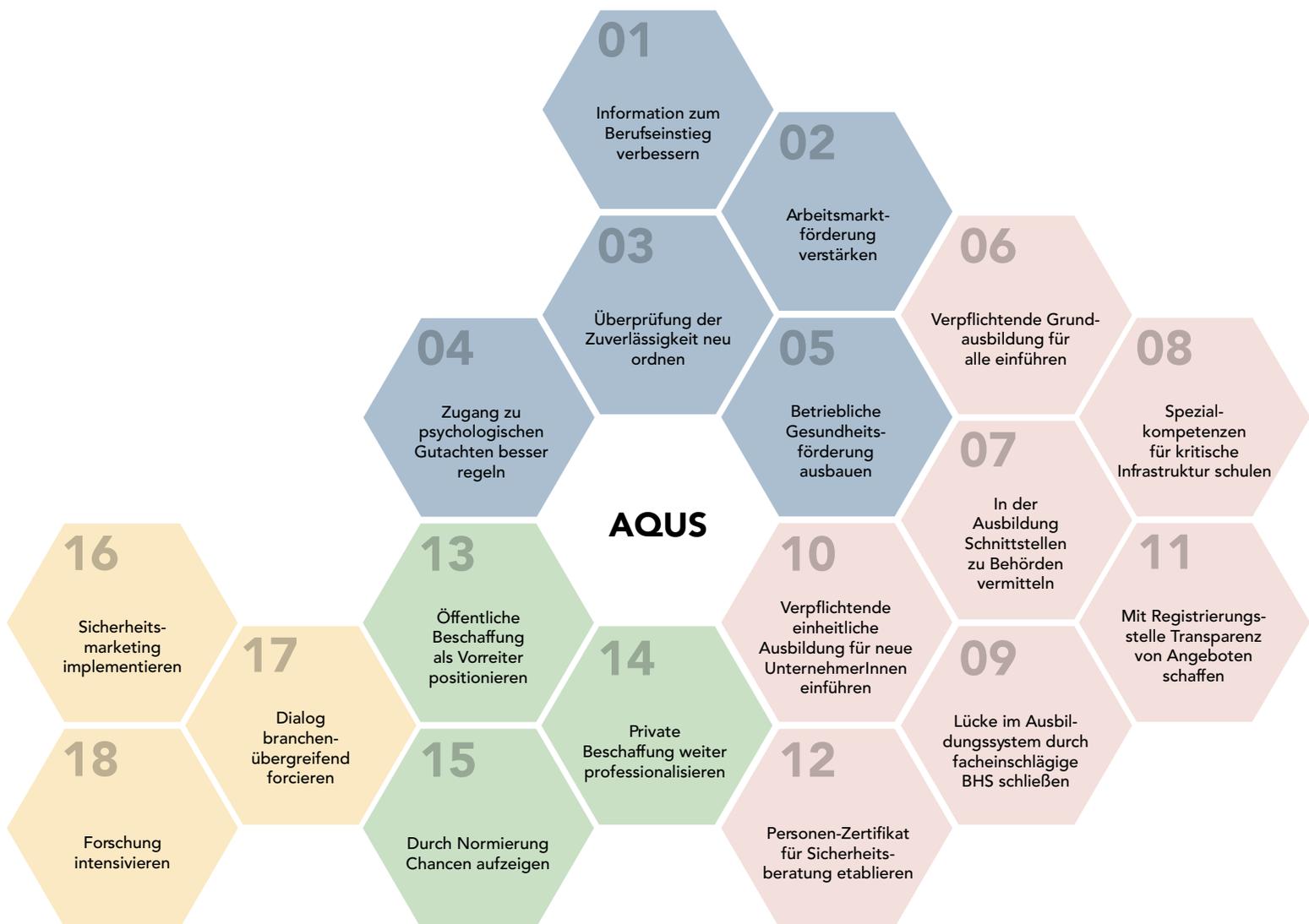
Die hier angeführten Empfehlungen basieren auf dem internationalen Vergleich, den Ergebnissen der explorativen Interviews mit VertreterInnen von SicherheitsdienstleisterInnen, der Leitfadeninterviews mit Stakeholdern und der Umfrage bei den Unternehmen bzw. Organisationen der kritischen Infrastruktur.

In der Folge wurden mehr als 40 mögliche Empfehlungen in vier Feedback-Gesprächen mit VertreterInnen der beteiligten Branchen und Institutionen zur Diskussion gestellt.

Die Empfehlungen stellen keinen Konsens der Beteiligten dar, sondern einen Vorschlag des Projektteams auf Basis der – mitunter sehr divergierenden – Rückmeldungen.

Sie gliedern sich in die vier Handlungsfelder

- A**    **Arbeitsmarkt und Arbeitsbedingungen**
- B**    **Aus- und Weiterbildung**
- C**    **Beschaffung und Normierung**
- D**    **Kommunikation und Bewusstseinsbildung**





**01**

Information zum  
Berufseinstieg  
verbessern

**02**

Arbeitsmarkt-  
förderung  
verstärken

**03**

Überprüfung der  
Zuverlässigkeit neu  
ordnen

**05**

Betriebliche  
Gesundheits-  
förderung  
ausbauen

**04**

Zugang zu  
psychologischen  
Gutachten besser  
regeln

## HANDLUNGSFELD A: ARBEITSMARKT UND ARBEITSBEDINGUNGEN

### 01 Information zum Berufseinstieg verbessern

Entwicklung und Publikation von freiwilligen Orientierungs- und Eignungstests für unterschiedliche Einsatzformen im Sicherheitsgewerbe, die online zur Verfügung stehen.

Mögliche Inhalte sind neben Arbeitsbedingungen in verschiedenen Verwendungen auch der Umgang mit Gefahren, Aufmerksamkeit, Lernen und Motivation. BewerberInnen kommen dadurch mit klareren Vorstellungen in Bezug auf die Anforderungen zu den Unternehmen.

Die Gestaltung dieser Tests sollte gendersensibel erfolgen, um den Beschäftigungschancen von Frauen Rechnung zu tragen.

Außerdem sollte auch eine Einstufung von Sprachkenntnissen (Verstehen, Sprechen, Lesen, Schreiben, nach europäischem Referenzrahmen) umfasst sein.

Rückmeldungen zu Erfahrungen von Bewachungsunternehmen und aus Kundenprojekten können in die laufende Verbesserung dieses Tests einfließen.

### 02 Arbeitsmarktförderung verstärken

Die Beratung von Arbeitssuchenden über Berufschancen im Sicherheitsgewerbe sollte ausgebaut werden. Damit einhergehend könnten Förderungen für hochwertige Ausbildungs- und Umschulungsmaßnahmen durch das AMS ausgebaut werden (vertiefende Fachausbildung für Sicherheitsaufgaben als arbeitsmarktnahe Qualifizierung bzw. Qualifizierungsförderung für Beschäftigte, aber auch vorbereitende Sprachkurse).

Außerdem wird ein laufender Dialog von BranchenvertreterInnen mit dem AMS (auf Bundes- und Landesebene) empfohlen.

### 03 Überprüfung der Zuverlässigkeit neu ordnen

Künftig sollten Überprüfungen der Zuverlässigkeit nach § 130 GewO bundesweit einheitlich erfolgen (inkl. Abgleich mit der „Gefährderliste“ und weiteren Datenbanken). Die grundsätzlichen Kriterien der Überprüfung sollten im Sinn der Transparenz und Vertrauensbildung für das Sicherheitsgewerbe veröffentlicht werden.

Das entsprechende Verfahren sollte für Unternehmen einfach und rasch auf elektronischem Weg abgewickelt werden können (nach Möglichkeit aber auch für InteressentInnen an einem Berufseinstieg). Jene Personen, bei

denen die Zuverlässigkeit nicht gegeben ist, sollten informiert werden, ob es Möglichkeiten gibt, die Zuverlässigkeit wieder zu erlangen.

Die Überprüfung der Zuverlässigkeit sollte seitens der Behörden regelmäßig wiederholt werden und Unternehmen bei Verlust der Zuverlässigkeit aktiv benachrichtigt werden. Das bedarf auch der Aufnahme entsprechender Klauseln in Dienstverträge bei Beschäftigten im Sicherheitsgewerbe.

Für sämtliche MitarbeiterInnen von Unternehmen im Sicherheitsgewerbe sollten behördlich ausgestellte Dienstausweise eingeführt werden. Diese sollten verpflichtend sichtbar zu tragen sein, außer besondere Gründe sprechen dagegen.

Außerdem sollten Unternehmen bzw. Organisationen der kritischen Infrastruktur stärker von den Möglichkeiten der Sicherheitsüberprüfung durch die Behörden Gebrauch (nach §§ 55 ff. Sicherheitspolizeigesetz) machen; insbesondere, wenn die Beschäftigten Sicherheitsaufgaben übernehmen, die Aufgaben des Sicherheitsgewerbes entsprechen.

Anmerkung: Einige der hier angeführten Punkte sind aktuell im Rahmen der Diskussion über eine mögliche „ArbeitnehmerInnen-Eignungsverordnung (AEV)“ bereits angedacht.

### 04 Zugang zu psychologischen Gutachten besser regeln

Im Zug der Novellierung des Waffengesetzes ist eine Neuregelung der psychologischen Gutachten vorgesehen (Stand: Oktober 2018). Aus dem Projekt heraus wird empfohlen, dass der wiederholte Zugang zu PsychologInnen bei negativen Gutachten eingeschränkt werden soll.

### 05 Betriebliche Gesundheitsförderung ausbauen

Besonderer Fokus der betrieblichen Gesundheitsförderung sollte auf mögliche spezielle körperliche Anforderungen und mögliche gesundheitliche Belastungen (z.B. die Arbeitsbedingungen an Alleinarbeitsplätzen) gelegt werden. Dafür sollten verstärkt Information und Bewusstseinsbildung bei Beschäftigten und Unternehmen im Sicherheitsgewerbe und bei Unternehmen/Institutionen der kritischen Infrastruktur, die internes Personal für Sicherheitsaufgaben einsetzen, erfolgen.



06

Verpflichtende Grundausbildung für alle einführen

08

Spezialkompetenzen für kritische Infrastruktur schulen

07

In der Ausbildung Schnittstellen zu Behörden vermitteln

11

Mit Registrierungsstelle Transparenz von Angeboten schaffen

10

Verpflichtende einheitliche Ausbildung für neue UnternehmerInnen einführen

09

Lücke im Ausbildungssystem durch facheinschlägige BHS schließen

12

Personen-Zertifikat für Sicherheitsberatung etablieren

## HANDLUNGSFELD B: AUS- UND WEITERBILDUNG

### 06 Verpflichtende Grundausbildung für alle einführen

Rasche und lückenlose Einführung einer (derzeit in Plänen für eine einschlägige Verordnung vorgeschlagenen) verpflichtenden Grundausbildung für sämtliche Beschäftigte (Arbeiter wie Angestellte) in Bewachungsunternehmen und internes Personal, das in Unternehmen/Organisationen der kritischen Infrastruktur eingesetzt wird.

In der Folge sollte auch überprüft werden, ob das aktuell in kritischer Infrastruktur eingesetzte Sicherheitspersonal die Anforderungen der Grundausbildung erfüllt.

### 07 In der Ausbildung Schnittstellen zu Behörden vermitteln

Für Unternehmen des Sicherheitsgewerbes und Unternehmen bzw. Organisationen der kritischen Infrastruktur und Bildungseinrichtungen sollten VertreterInnen von Sicherheitsbehörden zur Verfügung stehen. Diese sollten in Aus- und Weiterbildungsmaßnahmen Schnittstellen (und Abgrenzungsfragen) bei Kompetenzen und Eingreifmöglichkeiten authentisch und anhand von konkreten Beispielen erklären.

### 08 Spezialkompetenzen für kritische Infrastruktur schulen

Der Einsatz bei kritischer Infrastruktur erfordert oft – neben besonderer Zuverlässigkeit und Sprachkenntnissen – vertiefte Kenntnisse, etwa in Zusammenhang mit Revierdienst, Alarmintervention, Veranstaltungssicherheitsdienst sowie öffentlichem Personen- und Nahverkehr.

Mögliche Themen für kompakte vertiefende Aus- und Weiterbildungsmodul für höher qualifiziertes Sicherheitspersonal (internes Personal oder Personal von Sicherheitsdienstleistern) sind etwa

- rechtliche Rahmenbedingungen, Grundrechte, Persönlichkeitsschutz und Verfahrensrecht,
- aufgabenspezifisches Verhaltenstraining,
- Beurteilung gesundheitlicher Risiken einer Gewaltanwendung,
- Einsatz von körperlicher Gewalt und von Waffen für das Handeln in Notwehr oder in Notstandssituationen (insb. rechtliche Rahmenbedingungen für Waffengebrauch),
- Umgang mit Widerstand leistenden oder gewaltbereiten Personen,
- Kommunikation im Einsatz (mit technischen Hilfsmitteln, mündlich, schriftlich),
- Melde- und Berichtswesen, Dokumentation,
- Bedienung von Sicherheitstechnik und Gefahrenmeldeanlagen,
- Feststellen, Melden und Reagieren bei Notfällen (allgemein),
- Zusammenarbeit mit Einsatzkräften/Behörden,
- Erste Hilfe („betrieblicher Ersthelfer“),
- Brandschutz („Brandschutzwart“),

- Sprachkenntnisse auf einem bestimmten Niveau (nach europäischem Referenzrahmen),
- Korruptionsbekämpfung,
- Psychologie/Konfliktmanagement,
- Sensibilisierung für IT-Sicherheit, insb. auf privaten Smartphones und Tablets und
- Diversität und interkulturelle Kompetenz.

Daraus kann sich mittelfristig ein Berufsbild „Sicherheitsfachkraft für kritische Infrastruktur“ entwickeln.

Einzelne Qualifikationen (z.B. bei Erster Hilfe und Brandschutz) sind bereits heute in bestimmten Zeiträumen zu wiederholen. Bei den in der Aufzählung angeführten Spezialmodulen könnte eine derartige Regelung in einzelnen Fällen ebenfalls sinnvoll sein. Grundsätzlich wird empfohlen, dass Kursangebote und/oder Schulungsunternehmen zertifiziert und damit qualitätsgesichert sein sollen.

### 09 Lücke im Ausbildungssystem durch Einrichtung fach einschlägiger BHS schließen

Die Einführung einer Ausbildungsmöglichkeit im sekundären Bereich im Rahmen von berufsbildenden mittleren und höheren Schulen wäre anzustreben. Entsprechende Pläne werden etwa im BMLV bereits verfolgt. Die Einbindung von Unternehmen des Sicherheitsgewerbes wird bei solchen Initiativen sowie der existierenden Hochschuleinrichtungen jedenfalls empfohlen.

### 10 Verpflichtende einheitliche Ausbildung für neue UnternehmerInnen einführen

Zur Sicherstellung einer bundesweit einheitlichen Qualität im Sicherheitsgewerbe wäre eine verpflichtende Ausbildung (Vorbereitungskurs) vor Antritt zur Befähigungsprüfung angebracht. Inhaltlich und in Bezug auf den Umfang kann man sich an bestehenden Kursen (z.B. WIFI), der geplanten BHS und dem Beispiel Deutschlands orientieren.

### 11 Mit Registrierungsstelle Transparenz von Angeboten schaffen

Bei der Registrierungsstelle, die beim Allgemeinen Fachverband des Gewerbes in der Wirtschaftskammer Österreich eingerichtet wird, sollten künftig sämtliche formalisierten Schulungs- und Kursangebote in der Aus- und Weiterbildung (unternehmensintern wie extern) registriert werden und laufend aktuell abrufbar sein. Dabei sollten auch die Zertifizierungen der anbietenden bzw. eingesetzten Kursangebote und Schulungsunternehmen erfasst sein.

### 12 Personen-Zertifikat für Sicherheitsberatung etablieren

Entwicklung einer kompakten Ausbildung, gefolgt von einer freiwilligen Zertifizierung für UnternehmensberaterInnen, IT-DienstleisterInnen und UnternehmerInnen des Sicherheitsgewerbes als „zertifizierte/r SicherheitsberaterIn“.

## HANDLUNGSFELD C: BESCHAFFUNG UND NORMIERUNG

### 13 Öffentliche Beschaffung als Vorreiter positionieren

Entwicklung und Etablierung eines „Good-Practice“-Modells für die Beschaffung von Sicherheitsdienstleistungen im Sinne der Stärkung des Bestbieterprinzips nach dem Bundesvergabegesetz.

Im Zuge dessen sollte die Beratung von Unternehmen und Organisationen, die Sicherheitsdienstleistungen ausschreiben, ausgebaut werden und Ausschreibungen auf mögliche fachfremde Barrieren (wie etwa Umsatzhöhen etc.) bei Eignungs-, Auswahl- und Zuschlagskriterien überprüft werden. Außerdem sollte evaluiert werden, ob hier Möglichkeiten innovationsfördernder Beschaffung und Co-Entwicklung bestehen.

### 14 Private Beschaffung weiter professionalisieren

Sensibilisierung von Unternehmen und Organisationen der kritischen Infrastruktur für die Kompetenzen des Sicherheitsgewerbes (BerufsdetektivInnen und Bewachung) und mögliche Qualitätsaspekte bei der Beschaffung von Sicher-

heitsdienstleistungen, insbesondere der Kompetenz des eingesetzten Personals. Dabei kann man sich an der DIN 77200 bzw. dem COESS-Handbuch „Auftragsvergabe für qualitätsvolle private Sicherheitsdienstleistungen“ orientieren.

### 15 Durch Normierung Chancen aufzeigen

Das Projektteam regt an, dass Austrian Standards eine ÖNORM oder ON-Regel entwickelt, die eine Empfehlung für Mindestanforderungen für SicherheitsdienstleisterInnen bei kritischer Infrastruktur beschreibt. Hier könnte die Schweiz als Vorbild dienen, in der eine „Verordnung über den Einsatz von Sicherheitsunternehmen (VES)“ allgemeine Mindestvoraussetzungen für den Einsatz privater Sicherheitsfirmen definiert. Darin werden ein Verhaltenskodex, nachgewiesene Ausbildung der Beschäftigten, eine verpflichtende Haftpflichtversicherung etc. normiert.

Eine solche Norm könnte künftig in einschlägigen Beschaffungsvorgängen herangezogen werden.

13

Öffentliche  
Beschaffung  
als Vorreiter  
positionieren

14

Private  
Beschaffung weiter  
professionalisieren

15

Durch Normierung  
Chancen aufzeigen

## HANDLUNGSFELD D: KOMMUNIKATION UND BEWUSSTSEINSBILDUNG

### 16 Sicherheitsmarketing implementieren

Empfohlen wird eine gemeinsame, verstärkte und umfassende Bewusstseinsbildung für den hohen gesellschaftlichen Wert von Sicherheit als Faktor für ausgezeichnete Lebensqualität und einen erfolgreichen Wirtschaftsstandort durch Politik, Verwaltung, Unternehmen und Zivilgesellschaft.

Alle sind hier gefordert, ihren Beitrag zu leisten. Insbesondere bestehende Kooperationsplattformen von öffentlicher Hand und Unternehmen sollten das Thema künftig verstärkt aufgreifen und die Wertschätzung aller Personen, die im Bereich der Sicherheit arbeiten, ausbauen.

### 17 Dialog branchenübergreifend forcieren

Bestehende Informations- und Dialogplattformen sollten ausgebaut und um VertreterInnen aus dem Sicherheitsgewerbe, aus Hochschulen und der Zivilgesellschaft sowie weitere ExpertInnen inhaltlich verbreitert werden.

Dazu sollte ein regelmäßiger „Chancen- und Risikodialog“ als freiwilliges, offenes Austauschformat gemeinsam mit dem BMI/BVT und dem BMLV veranstaltet werden.

Mögliche Themen: Aus- und Weiterbildungsfragen inkl. Lehrpersonal, Information und Bewusstseinsbildung für einschlägige Normen und Methoden im Risiko- und Sicherheitsmanagement, sowie „Lessons learned“ zu Ausrüstung, digitaler Dokumentation etc.

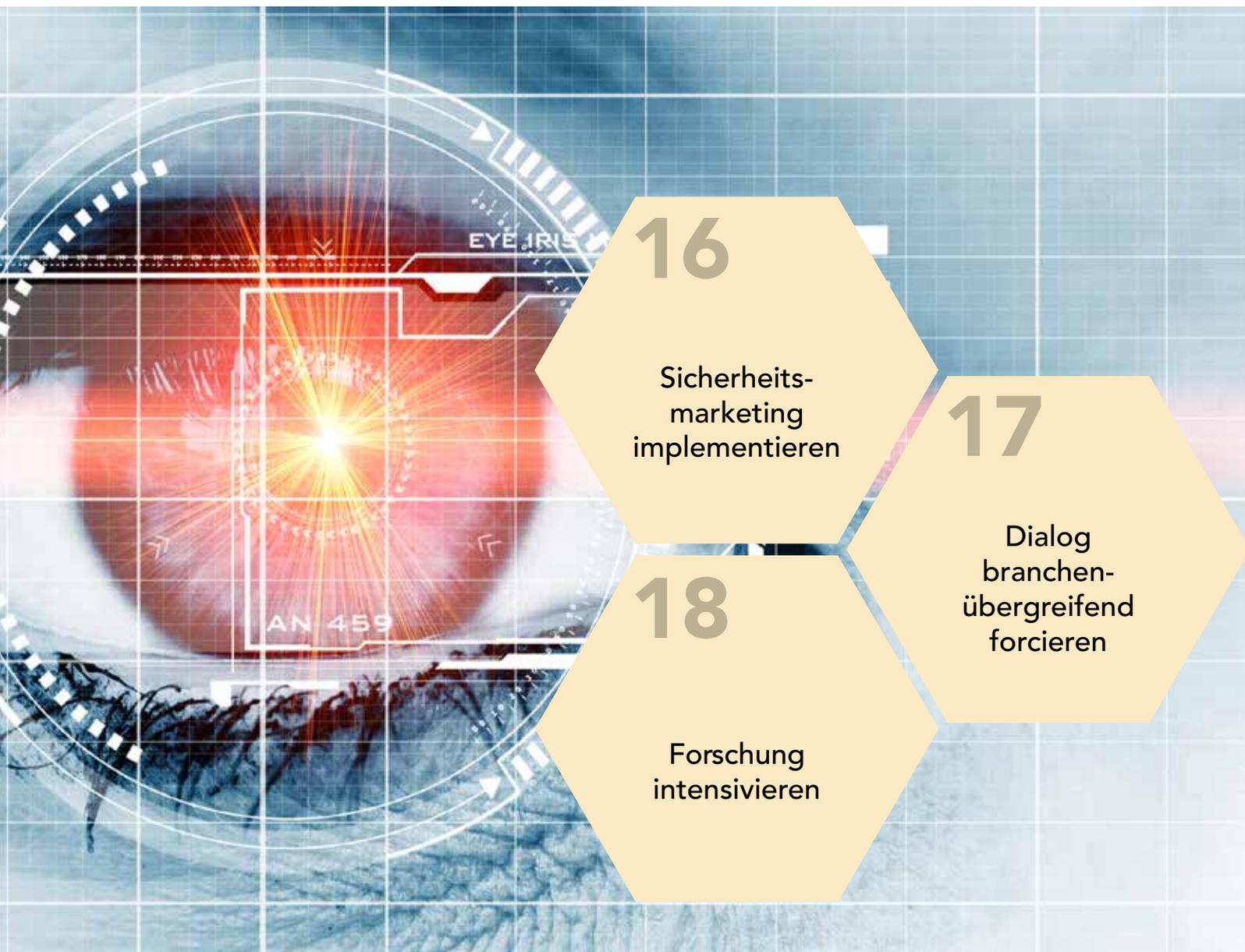
Darüber hinaus können die Vernetzung und der branchenübergreifende Wissensaustausch unter Unternehmen, die sich mit Beratung in Sicherheitsfragen befassen, ausgebaut werden.

### 18 Forschung intensivieren

Forschung im Themenbereich „Sicherheit bei kritischen Infrastrukturen“ kann relevantes Wissen generieren und die Entwicklung von Lösungen fördern.

Im Projekt AQUUS wurden folgende Themen aufgeworfen, die weiterer Untersuchungen bedürfen:

- konkreter Bedarf der kritischen Infrastruktur,
- Sammlung und (anonyme) Auswertung konkreter Vorfälle sowie Ableitung von Lösungsansätzen,
- internationale Trends, Entwicklungen am Arbeitsmarkt etc.



# 16

Sicherheits-  
marketing  
implementieren

# 17

Dialog  
branchen-  
übergreifend  
forcieren

# 18

Forschung  
intensivieren

## NACHWORT UND AUSBLICK

Trotz des allgemein sehr hohen Sicherheitsniveaus in Europa gibt es eine Reihe von Bedrohungen und Herausforderungen, denen sich die Gesellschaft stellen muss. Extremismus, Terrorismus wie auch die Digitalisierung erzeugen neue Bedrohungsbilder und Angriffsformen. In diesem Forschungsprojekt wurden Empfehlungen für Ausbildungs- und Qualitätsstandards für SicherheitsdienstleisterInnen formuliert, deren Umsetzung einen Beitrag zu einem höheren Sicherheitsniveau leisten soll.

Auch wenn ein Fokus auf dem Schutz von Unternehmen und Organisationen kritischer Infrastruktur liegt, können die Ergebnisse (und vor allem die Umsetzung der Empfehlungen) positive Auswirkungen auf die österreichische Gesellschaft als Ganzes haben: Einerseits erhöht der bessere Schutz der Unternehmen und Organisationen der kritischen Infrastruktur auch die allgemeine Sicherheitslage. Andererseits ist die Signalwirkung dieser Unternehmen und ihre Marktmacht bei der Nachfrage nach Sicherheitsdienstleistungen durch die Gestaltung von Ausschreibungen nicht zu unterschätzen.

Unabhängig von der Einführung von verpflichtenden (Mindest-)Standards für die Ausbildung von Beschäftigten bei Unternehmen des Sicherheitsgewerbes wird die Frage der Qualifikation des eingesetzten Personals noch stärker zur Schlüsselfrage am Markt werden. Der wichtigste Grund dafür ist die laufende Digitalisierung, die auch sämtliche Beteiligte in den Sicherheitsbranchen erfasst. Es ist zu erwarten, dass Automatisierung, Sensorik und künstliche Intelligenz zu neuen und vernetzten Lösungen zur Überwachung von Objekten führen – man denke nur an die Einsatzmöglichkeiten von Drohnen oder bodengebundenen mobilen Überwachungssystemen. Dass diese selbst dann wieder besondere Herausforderungen hinsichtlich IKT-Sicherheit mit sich bringen, sei hier nur kurz erwähnt.

Angesichts dieser zunehmenden Vernetzung von Online- und Offline-Welt wird der im Sicherheitsbereich beschäftigte „Faktor Mensch“ noch stärker mit der Überwachung und Steuerung von automatisierten Anlagen und Systemen, und der persönlichen Einschätzung von Situationen beschäftigt sein. Die Kommunikation (mit z.B. Kundinnen und Kunden, Beschäftigten, Gästen, Behörden etc.) wird voraussichtlich einen noch größeren Schwerpunkt darstellen. Das wird Berufsbilder verändern und jedenfalls intensiverer Aus- und Weiterbildung bedürfen.

Das breite Themenfeld Sicherheit allgemein braucht mehr öffentliche Aufmerksamkeit in Österreich und Europa – in Politik, Wirtschaft und Zivilgesellschaft. Mehr Wissen und Bewusstsein in der Bevölkerung können allgemein zu mehr Verständnis für Sicherheitsfragen und in besonderen Situationen zu besseren Einschätzungen und Reaktionen führen.

Daneben braucht es auch den laufenden offenen Austausch von allen, die in Behörden, Unternehmen und in Dienstleistungsberufen professionell Sicherheitsaufgaben wahrnehmen, um die Sicherheitskultur in diesem Land weiterzuentwickeln.

Abschließend sei noch erwähnt, dass die hier skizzierten Herausforderungen auch neuen Forschungsbedarf mit sich bringen werden.

Die in diesem Projekt formulierten Empfehlungen sollen einen kleinen Beitrag dazu leisten, dass Österreich weiterhin eines der sichersten Länder der Welt bleibt.

## DAS AQUUS TEAM

### Projektleitung



Luiza Putu

#### DI (FH) Mag. Thomas Goiser MBA MA

Unternehmens- und PR-Berater in Böhmekirchen und Wien, eingetragener Mediator, Autor und Lehrbeauftragter (u.a. an der FH Campus Wien sowie der Donau Universität Krems). Absolvent u.a. des Studiums der Rechtswissenschaften und des Masterstudiengangs Risk Management & Corporate Security an der FH Campus Wien. Frühere Karrierestationen bei Pléon Publico (Senior Consultant) sowie der Industriellenvereinigung im Bereich Marketing & Kommunikation.



FH Campus Wien Schedl

#### FH-Prof. Mag. Claudia Körmer

Lehrt und forscht seit 2014 im Fachbereich Risiko- und Sicherheitsmanagement der FH Campus Wien. In dieser Position war sie bereits für Studienprojekte wie z.B. „Konzernsicherheit in der D-A-CH Region 2016“ und „Wirtschafts- und Industriespionage in österreichischen Unternehmen 2015“ verantwortlich. Die Absolventin der Universität Wien (Soziologie und Philosophie) war davor als Projektleiterin im Kuratorium für Verkehrssicherheit tätig.  
*claudia.koermer@fh-campuswien.ac.at*

### Weiters im Projektteam



FH Campus Wien Schedl

#### FH-Prof. DI Dr. Martin Langer

Seit 2008 Leiter des Fachbereichs Risiko- und Sicherheitsmanagement der FH Campus Wien und der dort angesiedelten Studiengänge „Integriertes Sicherheitsmanagement“ (Bachelor) sowie „Integriertes Risikomanagement“ (Master). Davor war Langer als Berater für Sicherheits- und Krisenmanagement Österreich und Deutschland tätig. Zusätzlich war er leitend im Rahmen internationaler Einsätze für das Rote Kreuz, das österreichische Bundesheer und die UNO nach Naturkatastrophen in der Türkei, Mosambik, Honduras und dem Iran tätig. Langer ist Absolvent des Strategischen Führungslehrganges der österreichischen Bundesregierung.  
*martin.langer@fh-campuswien.ac.at*



DUK Andrea Reischer

#### Bettina Pospisil, MA, BA

Wissenschaftliche Mitarbeiterin im Zentrum für Infrastrukturelle Sicherheit an der Donau-Universität Krems mit den Forschungsschwerpunkten Infrastruktursicherheit, Cybersecurity, Cybercrime und Autonome Systeme. Vor ihrer Tätigkeit an der Donau-Universität Krems war die Soziologin als wissenschaftliche Mitarbeiterin an der Alpen Adria Universität Klagenfurt und an der WU-Wien sowie als Journalistin tätig.  
*bettina.pospisil@donau-uni.ac.at*



DUK

#### Ass.-Prof. Mag. Dr. Walter Seböck, MAS, MSc, MBA

Leiter des Zentrums für Infrastrukturelle Sicherheit sowie Assistenzprofessor für Security Studies an der Donau-Universität Krems mit den Forschungsschwerpunkten Sicherheitspolitik, Infrastruktursicherheit, E-Government, Cybersecurity, Big Data und Autonome Systeme. Der promovierte Politologe und Gründungsdekan der Fakultät für Wirtschaft und Recht verfügt über langjährige Erfahrungen in Führungspositionen als Verlagsleiter, Marketingleiter, Unternehmensberater, kaufmännischer Direktor und Geschäftsführer von Online-Agenturen und Online-Plattformen. Lektor an internationalen Universitäten wie z.B. an der Moskauer Lomonosov Universität und an der Hebei Universität, China.  
*walter.seboeck@donau-uni.ac.at*



DUK Andrea Reischer

#### Mag. Dr. Ingeborg Zeller

Lehrgangsleiterin des Security and Safety Management MSc-Programmes und Lehrgangskoordinatorin für nationale und internationale Corporate Programs im Zentrum für Infrastrukturelle Sicherheit an der Donau-Universität Krems. Leiterin der jährlichen Sicherheitskonferenz Krems. Ihr Forschungsschwerpunkt umfasst Infrastruktursicherheit, Objektsicherheit und Autonome Systeme. Die promovierte Betriebswirtin verfügt über langjährige Erfahrung im Weiterbildungsbereich mit Schwerpunkt Executive Education.  
*ingeborg.zeller@donau-uni.ac.at*



SecureLINE

#### Michael Zoratti, MSc.

Er ist seit 1976 im Sicherheitsmanagement tätig und seit 1998 geschäftsführender Gesellschafter der SecureLINE GmbH – Bildungszentrum SICHERHEIT, diplomierter Lebens- und Sozialberater, eingetragener Mediator, „Master of Science“ in Health Care Management, Vorstandsmitglied des KSÖ - Kuratorium Sicheres Österreich, Mitglied der wissenschaftlichen Beiräte der Universitätslehrgänge „Security & Safety Management“ und „Fire Safety Management“ an der Donau-Universität Krems, Vorsitzender des Komitees für Stadien, Sicherheit und Fans des ÖFB - Österreichischer Fußballbund und Autor zahlreicher Publikationen im Sicherheitsbereich.  
*michael.zoratti@secureline.at*

## PROJEKTKONSORTIUM



## UNSERE PARTNER

 Bundeskanzleramt

 Bundesministerium Inneres

 Bundesministerium Landesverteidigung

